

**UNIVERSIDAD DON BOSCO
VICERRECTORÍA ACADÉMICA
FACULTAD DE INGENIERÍA**



**TRABAJO DE GRADUACIÓN PARA OPTAR AL GRADO DE
Maestro(a) en Seguridad y Gestión de Riesgos Informáticos**

PROYECTO

Seguridad de Blockchain y sus usos futuros

PRESENTADO POR

Juan José Alas Castillo

José Reynaldo Trejo Valdez

Horacio Aquiles Quiteño Gutiérrez

ASESOR

Mg. Iván Orlando Alvarado Niño

Antiguo Cuscatlán, La Libertad, El Salvador, Centro América

Julio 2022

Tabla de Contenido

INTRODUCCIÓN.....	i
1. CAPÍTULO 1	1
1.1. Planteamiento del Problema.....	1
1.2. Objetivos	1
1.2.1. Objetivo General	1
1.2.2. Objetivos Específicos	1
1.3. Alcance.....	1
1.4. Limitaciones	1
2. CAPÍTULO 2	2
2.1. Marco Referencial	2
2.1.1. Introducción al Blockchain	2
2.1.2. ¿Qué es Blockchain?.....	2
2.1.3. Principales Características del Blockchain	3
2.1.4. Tipos de Blockchain	3
2.2. Marco Legal y Normativo	5
2.2.1. Constitución de la Republica de El Salvador	7
2.2.2. Ley Bitcoin. Decreto 57 – Asamblea Legislativa.....	7
2.2.3. Normas técnicas para facilitar la aplicación de la Ley Bitcoin – Banco Central de Reserva de El Salvador	8
2.2.4. NRP-29. Normas técnicas para facilitar la participación de entidades financieras en el ecosistema Bitcoin - BCR	9
2.2.5. Lineamientos para la autorización del funcionamiento de la plataforma de la billetera digital para Bitcoin y dólares.....	9
3. CAPÍTULO 3	11
3.1. Metodología de la investigación	11
3.1.1. Tipo de Investigación.....	11
3.1.2. Procedimiento	11
4. CAPÍTULO 4	14
4.1. Análisis e Interpretación de Resultados	14
4.1.1. Entornos de uso de Blockchain.....	14
4.1.2. Componentes de Blockchain	23
4.1.3. Situación Actual, Ventajas y Desventajas.	32
5. CAPÍTULO 5	37

5.1.	Propuesta de Uso	37
6.	CAPÍTULO 6	39
6.1.	Conclusiones y Recomendaciones.....	39
6.1.1.	Conclusiones	39
6.1.2.	Recomendaciones	40
7.	REFERENCIAS BIBLIOGRÁFICAS	41
8.	ANEXOS.....	44

Índice de ilustraciones

Ilustración 1	Ejemplo de Blockchain ilustrada en (10).....	25
Ilustración 2	Vista en alto nivel de una red Blockchain (37).....	26
Ilustración 3	Modelo de referencia propuesto por Andreas Ellervee (38)	27
Ilustración 4	Imagen de Referencia.....	37

Índice de Tablas

Tabla 1	Instrumentos de Análisis Objetivo 1	12
Tabla 2	Instrumentos de Análisis Objetivo 2	12
Tabla 3	Instrumentos de Análisis Objetivo 3	13
Tabla 4	Entornos de Adopción de Blockchain	14
Tabla 5	Entornos de uso Blockchain.....	14
Tabla 6	Componentes de Blockchain	23
Tabla 7	Seguridad y Privacidad del Blockchain.....	23
Tabla 8	Variables de Entorno en el uso actual de Blockchain	32
Tabla 9	Ventajas Tecnología Blockchain.....	32
Tabla 10	Desventajas Tecnología Blockchain	33
Tabla 11	Anexo 1 - Criterios de Adopción Blockchain	44
Tabla 12	Anexo 2 - Entornos de Uso Blockchain	44
Tabla 13	Anexo 3 - Componentes del Blockchain	44
Tabla 14	Anexo 4 - Seguridad y Privacidad del Blockchain.....	44
Tabla 15	Anexo 5 - Variables de entorno actual en el uso de Blockchain	44
Tabla 16	Anexo 6 - Ventajas uso Blockchain	45
Tabla 17	Anexo 7 - Desventajas uso Blockchain.....	45

RESUMEN

En un inicio, la tecnología Blockchain estuvo asociada a las billeteras electrónicas específicamente ligadas al Bitcoin. Sin embargo, en la actualidad esta tecnología puede ser utilizada para otros fines.

Los problemas que promete resolver y la idea detrás de Blockchain, ha despertado interés en diferentes ámbitos de la sociedad. Pero, la complejidad intrínseca y el dinamismo característico de esta tecnología, aun relativamente nueva, se presentan como obstáculos en la toma de decisión si el Blockchain es solución a un problema a resolver y en caso de serlo, qué implementación resulta apropiada para su construcción.

En esta investigación se analizan los beneficios del uso e implementación de Blockchain a la seguridad (disponibilidad, integridad y confidencialidad) de la información contrastado con los ámbitos actuales, para ello se elabora un documento que contiene los aspectos más importantes a considerar al momento de adoptar esta tecnología.

INTRODUCCIÓN

Esta investigación proporciona al lector una idea más clara de cómo la tecnología Blockchain está formada, la seguridad que se utiliza y como está siendo utilizada en la actualidad por ciertos sectores así mismo dar a conocer los usos y servicios que proveerá en un futuro cercano, las ventajas y desventajas de adopción de esta tecnología como solución a problemas actuales en diferentes rubros o sectores del mundo financiero, logístico, legal, productivo, salud entre otros.

El capítulo uno destaca las Generalidades del trabajo de investigación, el planteamiento del problema, objetivos, alcance, limitaciones y delimitaciones de este trabajo de investigación.

El segundo capítulo contempla el marco referencial, es decir la contextualización de la tecnología de Blockchain, características y tipos; a su vez se hace un repaso por el marco legal y normativo que se relaciona con la tecnología de cadenas de bloques.

En el capítulo tres se aborda la metodología de la presente investigación y el procedimiento utilizado en la investigación realizada.

El capítulo 4 muestra en detalle el análisis e interpretación de los resultados de la investigación, el análisis aborda cada uno de los objetivos y los hallazgos encontrados basado en la metodología antes planteada.

El capítulo 5 expone una propuesta de uso de la tecnología Blockchain mas allá de su uso tradicional como libro de registro o libro de mayor para criptoactivos, explorando su uso en otros ámbitos profesionales.

Finalmente, el capítulo 6 muestra las conclusiones y recomendaciones a las que se han podido llegar como fruto del presente trabajo de investigación.

1. CAPÍTULO 1

1.1. PLANTEAMIENTO DEL PROBLEMA

En el mundo actual y globalizado en el cual casi todas las áreas de las organizaciones e instituciones utilizan sistemas de información para almacenar datos, que a su vez son procesados para ser transformados en información, existe un riesgo muy alto de que esta información caiga en manos equivocadas teniendo en cuenta que gran parte de estas transacciones son realizadas por sistemas conectados a internet, lo cual los convierte en un blanco muy atractivo para los ciberdelincuentes teniendo un impacto negativo en la seguridad y privacidad de las personas.

Por ello surge la necesidad de adoptar nuevas tecnologías tales como el Blockchain para garantizar un acceso a la información de forma segura y que a su vez añada una capa extra de seguridad en el procesamiento, transporte y almacenamiento de datos dentro de los sistemas de información.

Dentro de los principales obstáculos por los cuales no se ha masificado el uso del Blockchain están los costos asociados como: la demanda de servidores con capacidades grandes de recursos que a su vez aumentan los consumos de energía eléctrica, la pérdida irrecuperable de la información al momento de extraviarse la llave pública quedando la información inaccesible, desarrollos de aplicaciones de usuario final para procesamiento y establecimiento de comunicación entre nodos.

1.2. OBJETIVOS

1.2.1. OBJETIVO GENERAL

Establecer documentación con los ámbitos y las tecnologías emergentes en el uso del Blockchain y su aplicación en el ámbito de seguridad informática.

1.2.2. OBJETIVOS ESPECÍFICOS

- Identificar los ámbitos de tecnologías que muestren una clara tendencia hacia la adopción del Blockchain.
- Identificar los principales componentes y mecanismos de seguridad de la tecnología Blockchain.
- Definir la situación actual del Blockchain, ventajas y desventajas.

1.3. ALCANCE

Dar a conocer los beneficios de la adopción de la tecnología Blockchain y los diferentes ámbitos en los que puede implementarse tales como: (a) financiero, (b) salud, (c) cadena de alimentación, (d) distribución y emisión de documentos personales entre otros. Así mismo identificar los aspectos mínimos necesarios para el funcionamiento de un entorno Blockchain.

1.4. LIMITACIONES

- Exploraciones adicionales limitadas sobre el uso e implementación de la tecnología Blockchain en ámbitos de uso fuera de los criptoactivos.
- Escasez de profesionales expertos en el área.
- Escasa de documentación y normativas técnicas sobre la tecnología Blockchain.

}

2. CAPÍTULO 2

2.1. MARCO REFERENCIAL

2.1.1. INTRODUCCIÓN AL BLOCKCHAIN

Blockchain es una innovación tecnológica que cuenta con la capacidad de transformar diversidad de sistemas tradicionales en sistemas mucho más seguros y autónomos, distribuidos, transparentes y colaborativos, mientras que empodera a sus usuarios (1). La tecnología Blockchain fue noticia por primera vez como base para nuevos tipos de transacciones financieras, comenzando con Bitcoin en 2009. Ya en los años 2020, una reconocida empresa de auditoría y consultorías PwC espera que los sistemas basados en Blockchain reduzcan o eliminen muchos puntos de fricción para una variedad de transacciones comerciales; las personas y las empresas podrán intercambiar una amplia gama de activos y valores digitalizados o representados digitalmente con cualquier otra persona. (2)

El creciente interés por el Blockchain y su potencial de brindar la confianza en ambientes donde los participantes no confían entre sí, ha motivado a diferentes empresas, organizaciones, y gobiernos a incluir Blockchain como parte de la solución a problemas existentes. Esto, a su vez, ha impulsado el desarrollo de diferentes herramientas que asistan en el desarrollo de aplicaciones distribuidas que utilizan Blockchain, es decir, plataformas de Blockchain.

2.1.2. ¿QUÉ ES BLOCKCHAIN?

Para el diccionario de Oxford, Blockchain es: “un sistema en el cual un registro de transacciones de Bitcoins u otras criptomonedas es mantenido en varias computadoras enlazadas entre sí en una red peer-to-peer”. Al analizar la definición, incorpora conceptos, que no se acoplan a esta investigación ya que su enfoque va más allá de su uso en criptomonedas.

Esta tecnología ha atraído la atención de instituciones como bancos, gobiernos y otras corporaciones comerciales convirtiéndose en una nueva frontera de capitales de riesgo.

Blockchain está a punto de convertirse en la invención más emocionante después de Internet; mientras que el segundo conecta el mundo a habilitar nuevos modelos comerciales basados en procesos en línea, el primero ayuda a resolver el problema de confianza de manera más eficiente a través de la computación en red¹.

2.1.3. PRINCIPALES CARACTERÍSTICAS DEL BLOCKCHAIN

- **Descentralización:** las transacciones pueden efectuarse entre pares de la misma sin necesidad de contar con la intervención de un tercero o autoridad central.
- **Inmutabilidad:** las transacciones se someten a un proceso de validación, confirmación, y almacenamiento distribuido en diferentes nodos pertenecientes a la red, de tal modo que resulta casi imposible modificar las transacciones almacenadas.
- **Auditabilidad:** consultando las transacciones almacenadas, participantes de la red y/o usuarios de aplicaciones que interactúan con la Blockchain pueden verificar y llevar una trazabilidad de registros almacenados.
- **Procedencia:** provee la forma de trazar el origen de cada transacción.
- **Red P2P:** los nodos participantes se comunican directamente entre sí, sin ninguna entidad ni nodo central o intermediario.
- **Base de datos distribuida:** cada nodo participante tiene acceso a una base de datos distribuida que ningún par individual controla y cualquiera de ellos puede verificarla o regenerarla en caso de ser necesario, sin ningún intermediario central.

2.1.4. TIPOS DE BLOCKCHAIN

Los tipos de Blockchain se pueden clasificar en función del acceso a los datos, la distinción entre los tipos de Blockchain es el esquema del libro distribuido y quién puede participar en el sistema. De esta manera tenemos Blockchain públicas, privadas e híbridas.

¹ Yan, Chen. *Blockchain tokens and the potential*. 2018.

Blockchain Públicas: son de tipo abierto, cualquiera puede participar. Los participantes acceden libremente a datos y realizan transacciones, pero debido a la falta de verificación de los participantes, se necesita de un cifrado y verificaciones avanzadas y, por lo tanto, la expansión de la red se torna lenta y difícil. El Blockchain público forma una perfecta estructura distribuida, y los participantes de la red son pseudoanónimos, por lo tanto, no es apropiado para los servicios financieros que necesitan ser controlados por la información centralizada de los sistemas de gestión (3). Una red pública de Blockchain está completamente abierta y distribuida; cualquiera puede unirse, participar y abandonar el sistema libremente. Por lo tanto, este sistema opera bajo nodos desconocidos y no confiables (4).

Blockchain Privadas: en este tipo el propietario genera y maneja el Blockchain. Esto es apropiado si el propietario desea administrar la Blockchain como el sistema centralizado. Los libros contables son compartidos y validados por un grupo predefinido de nodos. El sistema requiere iniciación o validación a los nodos que desean ser parte del sistema. Los nodos autorizados son responsables de mantener el consenso. Blockchain privadas son adecuadas para sistemas cerrados, donde todos los nodos son completamente confiables. En definitiva, es el propietario quien tiene la máxima autoridad para controlar el acceso a nodos autorizados.

Blockchain Híbridas: es el tipo intermedio de Blockchain pública y privada. A diferencia de Blockchain Privadas en el que el propietario tiene la autoridad, son los nodos preestablecidos quienes tienen la autoridad en este tipo de Blockchain. Por lo tanto, Blockchain Híbridas mantienen una estructura distribuida al mismo tiempo que fortalece la seguridad mediante una participación limitada, y resuelve el problema de la lenta velocidad de transacción y los problemas

de escalabilidad de la red planteados en Blockchain Pública. Por lo tanto, Blockchain Híbridas podrían ser utilizadas para transacciones entre instituciones financieras.²

2.2. MARCO LEGAL Y NORMATIVO

Ante los marcos jurídicos y regulatorios actuales el uso de la tecnología Blockchain por su naturaleza descentralizada puede conllevar algunas incertidumbres jurídicas, como tecnología, no se puede regular: solo se pueden regular las actividades que la utilizan. Sin embargo, existen retos regulatorios transversales que, independientemente del caso de uso específico, van a estar presentes y que tendrán que abordarse para facilitar su adopción, esto concluyó un estudio realizado en enero 2017 por el grupo financiero BBVA.

Principales retos regulatorios a los que se enfrenta Blockchain La falta de madurez de las iniciativas basadas en Blockchain y la fase experimental de los casos de uso identificados hacen que aún no exista una regulación específica de las actividades basadas en Blockchain en el sector de los servicios financieros. Algunas normas vigentes se aplicarán a los servicios basados en Blockchain: por ejemplo, los Smart Contracts asociados a esta tecnología al menos tendrán que cumplir con la normativa contractual aplicable en cada jurisdicción. Asimismo, dependiendo de los servicios financieros ofrecidos en el Blockchain (pagos, préstamos, inversiones, etc.), se tendrá que aplicar la normativa correspondiente. Sin embargo, si examinamos el panorama general del Blockchain, existen retos regulatorios transversales que tendrán que abordarse en algún momento en el futuro.

Inclusión de los proveedores de pagos y de transferencias internacionales que utilizan tecnologías Blockchain en las regulaciones sobre leyes contra el lavado de dinero y el

² Sunmola, Funlade T. y Apeji, Uje D. *Blockchain Characteristics for Sustainable Supply Chain*. 2020.

financiamiento del terrorismo con el fin de garantizar la igualdad de condiciones con los incumbentes y controlar los posibles usos ilícitos de las criptodivisas.

Marco jurídico relativo a la naturaleza legal de los Blockchain y los ledgers distribuidos que no están vinculados a una ubicación específica. En cuanto a la jurisdicción y la ley aplicable, la territorialidad constituye un problema, ya que cada nodo de la red puede estar sujeto a una ley diferente, y no hay una parte central cuya nacionalidad pueda servir como ancla normativa.

Marco jurídico para el reconocimiento de los Blockchain como fuentes únicas de verdad. Aunque existe un amplio consenso sobre la inmutabilidad de la información en un Blockchain bien definido, aún hay una falta de reconocimiento jurídico de esta inmutabilidad, por lo que aún no se puede utilizar como argumento válido en ningún tribunal. Un tema relacionado es el almacenamiento de la información de identidad en un Blockchain. El uso de Blockchains como fuentes únicas de identidad de confianza es el objetivo final de muchas partes interesadas y representaría un paso definitivo hacia una identidad digital universal, pero el reconocimiento de los Blockchains como fuentes inmutables de verdad es un requisito previo.

Normativa sobre cómo interpretar el “derecho al olvido”. La inmutabilidad del Blockchain podría colisionar con el derecho al olvido reconocido por algunas regulaciones sobre protección de datos. Esto podría lograrse mediante el cifrado automático de la información cuando se cumplan ciertas condiciones (usando un Smart Contracts, por ejemplo) o soluciones alternativas para evitar el acceso a esa información

Marco jurídico sobre la validez de los documentos almacenados en el Blockchain como prueba de posesión o existencia. Además del reconocimiento del Blockchain como una fuente única de verdad, hay un segundo nivel de reconocimiento necesario para ciertos negocios: que un documento almacenado en el Blockchain que representa la propiedad o la existencia de un activo realmente demuestre dicha propiedad o existencia. Si el proceso de verificar la veracidad

del documento antes de su inclusión en el Blockchain es lo suficientemente sólido, entonces el reconocimiento del Blockchain como una fuente inmutable de confianza implicaría el reconocimiento del documento como prueba de existencia o posesión. Una vez más, ningún tribunal en el mundo acepta esto todavía.

Marco jurídico para la información en Blockchain desde el punto de vista del flujo transfronterizo de datos y la protección de datos. La naturaleza compartida distribuida de los Blockchain tiene implicaciones directas en los datos almacenados. Aunque en los Blockchain públicos la información es accesible para todos los nodos de la red, en los ledgers federados es necesario gestionar con cuidado las porciones de información a las que accede cada participante. Asimismo, como ya se ha mencionado, también hay un problema de territorialidad que afecta a los datos. La información contenida en el ledger está descentralizada, por lo que hay un flujo transfronterizo de datos inherente que puede vulnerar las normativas existentes. (5)

2.2.1. CONSTITUCIÓN DE LA REPUBLICA DE EL SALVADOR

En la Constitución de la República de El Salvador en el artículo 131 numeral 13 menciona que “corresponde a la Asamblea Legislativa, Establecer y regular el sistema monetario nacional y resolver sobre la admisión y circulación de la moneda extranjera”; lo que da paso a que se apruebe desde dicho órgano del estado el uso del Bitcoin como moneda de curso legal

2.2.2. LEY BITCOIN. DECRETO 57 – ASAMBLEA LEGISLATIVA

De acuerdo al Decreto 57 aprobado por la Asamblea Legislativa de El Salvador se aprueba la Ley Bitcoin. La presente ley tiene como objeto la regulación del Bitcoin como moneda de curso legal, irrestricto con poder liberatorio, ilimitado en cualquier transacción y a cualquier título que las personas naturales o jurídicas públicas o privadas requieran realizar sin perjuicio de la aplicación de la Ley de Integración Monetaria. (6)

2.2.3. NORMAS TÉCNICAS PARA FACILITAR LA APLICACIÓN DE LA LEY BITCOIN – BANCO CENTRAL DE RESERVA DE EL SALVADOR

El Reglamento será aplicable a los Proveedores de Servicio de Bitcoin, el cual es definido como: Persona Natural o jurídica que provee para sí mismo o para terceros servicios relacionados con el Bitcoin, y de manera ejemplificativa se mencionan los custodios, Exchange y procesadores de pagos o billeteras.

Se crea el Registro de Proveedores de Servicios Bitcoin (el “Registro”), el cual estará a cargo del Banco Central de Reserva (“BCR”). El Registro será obligatorio para Proveedores de Servicios Bitcoin. Previo al inicio de operaciones deberán presentar al BCR el formulario de solicitud, escritura de Constitución y documentos de Identidad de los socios. Se deberá de presentar dentro de los 20 días hábiles siguientes a la entrada en vigencia del Reglamento (a más tardar 7 de octubre).

Se establece como normas de conducta con la que se deben de conducir los Proveedores de Servicio:

- Contar con un programa contra el lavado de dinero en cumplimiento con la legislación local y prácticas internacionales.
- Procedimientos para evitar pérdidas, robo o deterioro de los activos de los clientes.
- Registro de activos, pasivos y patrimonio del Proveedor de Servicios y registros de cuentas y transacciones de clientes, así como de los reclamos o quejas de estos últimos.
- Publicar en su página web y en los términos de la aplicación el contacto de la Superintendencia del Sistema Financiero para avocarse en caso de quejas no resueltas del proveedor.
- Programa de ciberseguridad.
- Programa de seguridad física y plan de recuperación de desastres (“BCP”).

- Plan de resolución que prevea liquidación ordenada en caso de insolvencia.
- Límite a las transacciones acorde a la gestión integral de riesgos.

La Superintendencia del Sistema Financiero será el ente encargado de la supervisión de la normativa aplicable a los sujetos obligados bajo la Ley Bitcoin. Adicionalmente establece que los Bancos están facultados (más no obligados), a prestar servicios financieros a los Proveedores de Servicios Bitcoin o abrir cuentas a usuarios Bitcoin. Sin embargo, los Bancos deberán prestar servicios, como plataformas de intercambio sin generar comisión, a las billeteras digitales ofrecidas por el Estado a fin de garantizar la inclusión financiera. (6)

2.2.4. NRP-29. NORMAS TÉCNICAS PARA FACILITAR LA PARTICIPACIÓN DE ENTIDADES FINANCIERAS EN EL ECOSISTEMA BITCOIN - BCR

El BCR crea las normas técnicas que tienen por objeto regular los sujetos que ofrezcan servicios basados en Bitcoin a sus clientes, ya sean personas naturales o jurídicas, y pudiendo estos servicios ser ofertados directamente o a través de un Proveedor de Servicios de Bitcoin. Los sujetos pueden participar en la prestación de servicios de billetera con custodia o sin custodia basados en Bitcoin, servicios de intercambio, procesamiento de pagos, entre otros servicios, así como ofrecer el conjunto completo de sus servicios bancarios a un Proveedor de Servicios de Bitcoin (7).

2.2.5. LINEAMIENTOS PARA LA AUTORIZACIÓN DEL FUNCIONAMIENTO DE LA PLATAFORMA DE LA BILLETERA DIGITAL PARA BITCOIN Y DÓLARES

El BCR crea lineamientos que tienen como objetivo establecer las disposiciones aplicables para la autorización del funcionamiento de las plataformas tecnológicas de los servicios con Bitcoin y dólares de los Estados Unidos de América, que deseen proveer los sujetos obligados a sus clientes, sean estos personas naturales o jurídicas. Estos serán de aplicación para los Bancos, Bancos Cooperativos, Sociedades de Ahorro y Crédito y Sociedades Proveedoras de Dinero Electrónico del país, que deseen proveer servicios con Bitcoin y dólares,

que para estos efectos serán denominados Administradores de Servicios con Bitcoin y dólares, en adelante Administradores. Los Administradores, podrán prestar servicios relacionados a Billeteras Digitales para Bitcoin y dólares, casas de intercambio digital o Exchange, plataformas, pasarelas o procesadores de pagos, entre otros. (8)

3. CAPÍTULO 3

3.1. METODOLOGÍA DE LA INVESTIGACIÓN

3.1.1. TIPO DE INVESTIGACIÓN

Debido al tema y su aplicación, la investigación se clasifica a partir de varios criterios y autores como Roberto Hernández Sampieri establece dos enfoques: cualitativo y cuantitativo, la presente investigación se corresponde con un enfoque cualitativo en relación al alcance de las investigaciones cuantitativas el presente estudio se clasifica como tipo descriptiva por su alcance de evidenciar los aspectos mínimos y condiciones que deben tomarse en cuenta a evaluar, abordando documentación bibliográfica utilizándola para la redacción del mismo.

3.1.2. PROCEDIMIENTO

El desarrollo de la guía metodológica tendrá como base en documentación técnica y artículos científicos, así como referencias a buenas prácticas de la seguridad de la información y sus propiedades.

Se analizará el material existente en las diferentes fuentes en el desarrollo de la investigación tales como fichas resúmenes y apuntes relevantes de las lecturas. Dada la naturaleza y los resultados esperados de la investigación, la principal técnica a utilizar será el análisis de contenidos lo que se llevará a cabo con la realización de sesiones síncronas, asíncronas, análisis de contenido, lluvia de ideas, controles de lectura y discusión de artículos.

Para desarrollar la idea principal se apoyó en los objetivos específicos planteados de la presente investigación.

Objetivo 1: Identificar los ámbitos de tecnologías que muestren una clara tendencia

hacia la adopción del Blockchain

Para la recolección de información que darán respuesta a este objetivo se utilizarán los siguientes instrumentos:

Tabla 1 Instrumentos de Análisis Objetivo 1

No	Unidades de análisis	Técnica de análisis	Instrumento
1	Tipo de información y cantidad de transacciones	Análisis de contenido	Tabla de criterios de entornos para adopción de Blockchain. Ver Anexo 1
2	Entornos de adopción de tecnología Blockchain	Análisis de contenido	Tabla de entornos de uso de Blockchain. Ver Anexo 2

Objetivo 2: Identificar los principales componentes y mecanismos de seguridad de

la tecnología Blockchain

Para la recolección de información que darán respuesta a este objetivo se utilizarán los siguientes instrumentos:

Tabla 2 Instrumentos de Análisis Objetivo 2

No	Unidades de análisis	Técnica de análisis	Instrumento
1	Componentes del Blockchain	Análisis de contenido	Lista de Componentes de Blockchain. Ver Anexo 3
2	Mecanismos de Seguridad del Blockchain	Análisis de contenido	Seguridad y Privacidad del Blockchain. Ver Anexo 4

Objetivo 3 Definir la situación actual del Blockchain, ventajas y desventajas

Para la recolección de información que darán respuesta a este objetivo se utilizarán los siguientes instrumentos:

Tabla 3 Instrumentos de Análisis Objetivo 3

No	Unidades de análisis	Técnica de análisis	Instrumento
1	Variables del Entorno Actual en el Uso de Blockchain	Análisis de contenido	Variables del Entorno Actual en el Uso de Blockchain. Ver Anexo 5
2	Ventajas de Tecnología Blockchain	Análisis de contenido	Ventajas Tecnología Blockchain. Ver Anexo 6
3	Desventajas de Tecnología Blockchain	Análisis de contenido	Desventajas de Tecnología Blockchain. Ver Anexo 7

4. CAPÍTULO 4

4.1. ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

4.1.1. ENTORNOS DE USO DE BLOCKCHAIN

Objetivo 1: Identificar los ámbitos de tecnologías que muestren una clara tendencia hacia la adopción del Blockchain

Tabla 4 Entornos de Adopción de Blockchain

Tabla de criterios de entornos para adopción de Blockchain		
No	Criterio	Descripción
1	Alto flujo de transacciones	Que la naturaleza del entorno obligue al mismo a realizar múltiples transacciones
2	Información confidencial	Que la información involucrada sea de carácter confidencial
3	Cantidad de actores Elevada	Que sus procesos involucren varios actores

Tabla 5 Entornos de uso Blockchain

Tabla de entornos de uso Blockchain	
Entornos	Descripción
Salud	Este es uno de los sectores en los que Blockchain soluciona el problema de la digitalización y resguardo de información sensible ya que por su seguridad esta información se mantendría íntegra y confidencial
Cadenas de suministros	Las alianzas estratégicas entre empresas y organizaciones tienen como objetivo incorporar la tecnología Blockchain a los procesos que componen la cadena de suministros y la utilización de esta en aplicaciones en torno a todos los procesos que la conforman desde la adquisición de materia prima hasta el destino final del producto.

Arte	Los derechos de autor y la autenticidad de obras de arte siempre ha sido un problema el cual ahora en día el sector arte está incorporando tecnología Blockchain para tener una trazabilidad y una fiabilidad de los productos, controlando fraudes y falsificaciones.
Filantropía	Las donaciones se pueden tratar como parte de una cadena de suministros, un problema muy recurrente es que cualquier tipo de bien que es donado, el donante no tiene las garantías del destino de estos, dando lugar a robos, perdidas, tanto de dinero como de los activos, por lo que Blockchain sería la solución.
Identidad	La validación de identidad es uno de los campos en los que la tecnología Blockchain podría evitar robo de identidad, fraudes y errores humanos al momento de su validación.
Financiero	Es el sector que más aceptación ha tenido, con la utilización de billeteras electrónicas, por lo que están incorporando Blockchain para adquirir y realizar préstamos ³ ; crowd-funding ⁴ , aseguradoras, entre otros.
Gobierno	Se presentan diferentes escenarios en los cuales a la utilización de Blockchain resulta de utilidad, entre ellos se encuentran: manejo de identidad, almacenamiento de documentos, sistema de votación, salud, Smart Cities, censos poblacionales.

Basados en el ámbito que más aceptación tiene a la tecnología del Blockchain siendo este el Bitcoin se puede decir con certeza que el área financiera con el consumo de transacciones digitales es el área con mayor adopción, dando paso a la implementación de dicha tecnología en diferentes áreas entre las cuales se puede mencionar: Registro Académico, Registros Médicos, Registro del Estado Civil, Validación de Respaldo de Datos las cuales presentan un común denominador que son las transacciones realizadas por los usuarios mediante el uso Blockchain.

³ **ETHLend**. [En línea] <https://ethlend.io/es>.

⁴ **Weifund**. [En línea] <http://weifund.io/>.

A continuación, se describen de manera más detallada los entornos de uso de la tecnología Blockchain, algunos ejemplos, contextos y casos de uso particulares en donde la adopción y aplicación de la tecnología Blockchain constituye una solución a problemas existentes. Los escenarios identificados se clasifican según el área al cual pertenecen:

Salud. Una de las posibles industrias o sistemas en los cuales puede incorporarse Blockchain es en el sector de la salud. Es conocido como uno de los sectores en los cuales la digitalización ha sido un proceso lento en comparación con adopciones en otras industrias, por varios motivos, uno de ellos debido a la sensibilidad de la información que en este ámbito se manipula. Además, la gestión de los servicios de salud y las partes involucradas pueden ser de suma complejidad dependiendo de las reglamentaciones de los diferentes países.

Existen actualmente algunas iniciativas que pretenden resolver algunos de los problemas en esta área utilizando Blockchain:

- **Pagos en el sistema de salud:** No es el caso de El Salvador, pero en países como Estados Unidos donde los servicios de salud se contratan en modalidad de seguros, los pagos de los mismos involucran a muchas entidades y pueden resultar de gran complejidad. Un seguro de salud puede ser utilizado en diferentes instituciones prestadoras de servicios y con estos se accede a un conjunto de servicios dependiendo del tipo de seguro que se obtenga, los pagos pueden realizarse a través de bancos, préstamos, entre otros. IBM Blockchain propone la utilización de Blockchain para resolver alguno de los problemas que el pago en los sistemas de salud implica entre los que se pueden mencionar: pagar a los proveedores y aseguradoras a tiempo, brindar servicios a pacientes cuando lo requieren, evitar un “doble registro” y acceder desde un solo sitio a la información completa de los pacientes
- **MedRec.** Esta iniciativa propone una nueva forma de almacenar historias clínicas electrónicas (HCE) utilizando Blockchain, con el objetivo de brindar a los pacientes un

registro inmutable de fácil acceso a las mismas. La plataforma resuelve el problema de la autenticación, confidencialidad, contabilidad y la posibilidad de intercambiar datos entre los prestadores de salud. (9).

- **PokitDok/DocChain.** DokChain es una red distribuida de nodos que procesan transacciones sobre datos clínicos e información financiera relativa a la industria de la salud. Tiene como objetivo aprovechar las ventajas que brinda la tecnología Blockchain involucrando a las diferentes partes interesadas para construir una nueva economía en la cual los datos y servicios en salud sean cuantificables e intercambiables; garantizando además la seguridad y privacidad de la información. (10) (11)

Cadenas de Suministro. Existen hoy en día numerosas alianzas entre diferentes empresas y organizaciones con el objetivo de incorporar la tecnología Blockchain a los procesos involucrados en las cadenas de suministro. Si bien las posibles aplicaciones entorno a estos procesos difieren, existen elementos que son comunes:

- La utilización de Blockchain en estos casos tiene como objetivo brindar transparencia al proceso, así como también agilizarlo. Se pretende además reducir la posibilidad de fraude u ocurrencia de errores, mejorar la administración de inventarios, minimizar los costos de traslados, identificar a los involucrados en el proceso, reducir demoras por papeleo.
- Respecto a la solución para registrar la trazabilidad de diferentes productos, objetos, activos involucrados, los proyectos expuestos proponen la utilización de sensores conectados a internet que permitan determinar en dónde y en manos de quién se encuentran los productos.
- Son proyectos piloto, acuerdos entre organizaciones y el acceso a información académica o formal respecto a su implementación en particular es escasa.
- Se propone la utilización de contratos inteligentes (Smart-Contracts) para definir reglas de negocio, estos son simplemente programas almacenados en una cadena de bloques

que se ejecutan cuando se cumplen condiciones predeterminadas. Por lo general, se utilizan para automatizar la ejecución de un acuerdo para que todos los participantes puedan estar seguros de inmediato del resultado, sin la participación de ningún intermediario ni pérdida de tiempo. También pueden automatizar un flujo de trabajo, activando la siguiente acción cuando se cumplen las condiciones.

A continuación, se detallan algunos ejemplos de este tipo de caso de uso:

- **Viant.** Es una plataforma de Blockchain, basada en Ethereum que, en conjunto con Microsoft Azure, lanzaron en diciembre 2019 un proyecto que tiene como objetivo, utilizando Blockchain, proveer un mecanismo que permita verificar paso a paso el trayecto del pescado desde que es capturado en el océano hasta que llega al plato de los consumidores⁵ (12)
- **Blockchain Food Safety Alliance.** IBM Blockchain Platform, Walmart, JD.com y la universidad de Tsinghua anunciaron en diciembre de 2018 un proyecto en el cual se pretende mejorar el tracking, la trazabilidad y la seguridad de los alimentos en China. Blockchain pretende ser utilizado para brindar información acerca de la trazabilidad de los alimentos en tiempo real. El grupo pretende cumplir sus objetivos involucrando a proveedores, reguladores de la industria y la comunidad científica, desarrollando protocolos y procesos que, utilizando Blockchain, brinden mayor transparencia al proceso. Existen actualmente pilotos de este proyecto, para registrar la trazabilidad del cerdo y el mango en China y en Estados Unidos y Walmart afirma que, la utilización de Blockchain para el proceso, ha reducido el tiempo necesario para rastrear mangos desde la granja hasta el supermercado (pasando de llevar días e incluso semanas a segundos). Similar a esta propuesta IBM ha anunciado colaboraciones con otras empresas de la

⁵ **Viant.** [En línea] <https://viant.io>.

industria alimenticia como son: Dole, Driscoll's, Golden State Foods, Kroger, McCormick and Company, McLane Company, Nestlé, Tyson Foods, Unilever and Walmart to Address Food Safety Worldwide (13).

- **IBM Blockchain and SAP IoT Solution for the Pharmaceutical Cold Chain.** Este proyecto pretende, utilizando Blockchain e IoT brindar una solución a la cadena de frío que debe mantenerse en la industria farmacéutica para determinados fármacos. Se propone utilizar sensores, conectados a internet que brinden información de los fármacos (ubicación, temperatura, etc.) y que dicha información sea registrada en un Blockchain en determinados eslabones de la cadena. Se propone la utilización de contratos inteligentes para establecer reglas de negocio. A modo de ejemplo, si el sensor de temperatura registra un valor superior a determinado umbral establecido el paquete debe ser inspeccionado y se asigna como responsable de las pérdidas al integrante de la cadena que registre temperaturas superiores al umbral. (14)
- **Insurwave.** Es una plataforma, construida sobre Corda (plataforma Blockchain), puesta en producción por EY, Guardtime, A.P.Moller-Maersk, Microsoft, Willis Towers Watson, XL Catlin, MS Amlin, y ACORD. Pretende que todas las partes accedan en tiempo “casi” real a la ubicación, condiciones y seguridad de los activos. (15) (16) (17)
- **TrustChain.** Es una colaboración que tiene el objetivo de utilizar IBM Blockchain Platform para registrar la trazabilidad de las joyas desde que se extraen hasta que son transformadas en una pieza final y entregadas a un punto de venta (18). Es por ahora una prueba de concepto, pero se espera su puesta en producción para fines de 2019.

Artículos académicos al respecto. “Towards an Ontology-Driven Blockchain Design for Supply Chain” (19): propone una ontología para el diseño de este tipo de sistemas. “Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT” (20). Se estudia la utilización de Blockchain e internet de las cosas y en especial, se propone un sistema de control de acceso

para dispositivos de IoT que permita escalar en escenarios donde este tipo de dispositivos abundan, como es el caso mencionado en este punto.

Arte. En la industria del arte y el entretenimiento ha existido desde sus inicios problemáticas relacionadas con el derecho de autor y la autenticidad. La utilización de la tecnología Blockchain en esta industria puede ser de especial utilidad para garantizar un intercambio de este tipo de bienes en dónde sus propietarios, así como también quienes crearon las piezas de arte (esculturas, pinturas, música, etc.) reciban la remuneración correspondiente según los derechos de autor, pudiendo evitar también casos de falsificación o piratería sin la necesidad de contar con un intermediario. A continuación, se detallan algunos ejemplos de este tipo de casos de uso:

- Una de las propuestas es la utilización de la tecnología Blockchain para llevar un registro de las transacciones de pinturas, esculturas, etc. de modo de conocer cuando estas están siendo exhibidas en exposiciones, a quién pertenecen, su origen, etc. (21) (22) (23). Como ejemplo de un proyecto en particular, se destaca Verisart (24). Verisart utiliza la tecnología Blockchain para generar certificados de autenticidad de las piezas de arte, verificar la proveniencia de las piezas, registrar a quién pertenecen y proteger la identidad de los propietarios, entre otros. Además, provee de una API para interactuar con la plataforma.
- **Ujo.** Este proyecto utiliza Blockchain para crear una base de datos de derechos y propiedad intelectual en la industria de la música. (25).

Filantropía. Otra de las posibles aplicaciones de la tecnología Blockchain, que se encuentra relacionada de cierto modo con las aplicaciones respecto a cadenas de suministro, son las donaciones. Es un problema conocido que en muchos casos quienes realizan donaciones no reciben garantías ni retroalimentación respecto al destino y distribución de sus contribuciones. En muchos casos, en circunstancias en las cuales se realizan donaciones ocurren robos,

pérdidas o los activos donados no tienen los destinos que deberían. IBM en conjunto con Global Citizen, lanzaron en mayo de 2018 el concurso “Challenge accepted” para construir una aplicación utilizando Blockchain que permita llevar un registro de las donaciones. La propuesta particular es construir una red con tres nodos: un gobierno, AID.org y GlobalCitizen en la cual las transferencias de fondos las realiza el gobierno, se registran con las organizaciones AID y se validan por parte de GlobalCitizen (26). Si bien esta propuesta pretende resolver una realidad acotada se espera que se desarrollen nuevos proyectos entorno a esta área.

Identidad. La validación de identidad es muy importante en el sector financiero. Identificar usuarios normalmente requiere el uso de canales físicos para demostrar ser quien dice ser, un usuario muestra algún tipo de documento de identidad, lo cual es ineficiente y propenso a errores. Instituciones financieras de Canadá reconocieron este problema y se asociaron con SecureKey Technologies para lanzar el servicio SecureKey Concierge, el cual permite a los usuarios autenticarse utilizando por ejemplo sus credenciales bancarias (27). Utilizando Hyperledger Fabric (plataforma Blockchain) se construyó una herramienta donde los bancos y otras empresas son proveedores de datos relacionados a la identidad de las personas tales como su nombre, número de documento, edad o puntaje crediticio, y los usuarios eligen cuándo y a quién mostrar atributos específicos de su identidad.

Sector Financiero. La tecnología Blockchain adquirió popularidad tras la publicación del artículo de Nakamoto en el cual presenta Bitcoin. Así como Bitcoin se han desarrollado diferentes sistemas de pago electrónico, sin embargo, este tipo de aplicaciones no es el único en el sector financiero. Existen, por ejemplo, aplicaciones para adquirir y realizar préstamos (28); crowdfunding (29), aseguradoras, entre otros.

Gobierno. En otros países la democracia líquida o democracia delegativa revocable es una forma de democracia directa que incluye la posibilidad de delegación de voto revocable de forma instantánea, de ahí su liquidez (30). Este tipo de sistemas puede ser implementado a través

de un sistema de tesorería. Un sistema de tesorería es un mecanismo de toma de decisiones colaborativo descentralizado y controlado por la comunidad para el financiamiento sostenible del desarrollo y mantenimiento de Blockchain. Durante cada período de tesorería, las propuestas de proyectos se envían, discuten y votan; los proyectos mejor calificados son financiados por el tesoro. El sistema de gobierno Dash (31) es un ejemplo del mundo real de ese tipo de sistemas (32). De esta forma Blockchain brinda soporte para la utilización de democracia líquida a aplicaciones que se construyan encima de la misma.

Una de las principales áreas en las cuales la tecnología Blockchain promete contribuir es en el desarrollo de aplicaciones para gobiernos (33). Se presentan diferentes escenarios en los cuales a la utilización de Blockchain resulta de utilidad, entre ellos se encuentran:

- Manejo de identidad y almacenamiento de registros (Se menciona el caso de Estonia, en donde se encuentran realizando un proyecto para otorgar residencias electrónicas).
- Almacenamiento de documentos (por ejemplo, partidas de nacimiento, certificados de votación, libretas de matrimonio, y demás trámites que al momento son entregados de forma física y presenciales.).
- Sistemas de votación para cualquier tipo de elección.
- Salud (almacenar las historias clínicas de modo que sean accesibles desde cualquier prestador de servicio, así como también contribuir en tareas de investigación publicando por medio de Blockchain registros anonimizados).
- Smart Cities, IoT, Censos Poblacionales.

4.1.2. COMPONENTES DE BLOCKCHAIN

Objetivo 2: Identificar los principales componentes y mecanismos de seguridad de la tecnología Blockchain

Tabla 6 Componentes de Blockchain

Componentes del Blockchain	
Componente	Descripción
Hash	Contiene información única asociada a la cadena anterior.
Bloque Genesis	Bloque inicial de la cadena, no contiene ninguna referencia de otros bloques.
Campo Nonce	Se utiliza para la creación del hash y la información de las cadenas sucesivas.
Nodos	Computadoras individuales por las que pasan o se realizan las transacciones.
Transacciones	Intercambio de información entre dos nodos
Actores	Divididos en dos: usuarios y Generador de bloques
Procesos	Serie de pasos ejecutadas en las transacciones
Servicios	Prestación de recursos distribuidos por la red

Tabla 7 Seguridad y Privacidad del Blockchain

Seguridad y Privacidad del Blockchain	
Mecanismo de Seguridad	Descripción
Mecanismos de Cifrados	Estrategias empleadas para la comunicación entre nodos.
Control de Acceso	Regula el nivel de acceso a las transacciones realizadas.

Consenso	Se refiere al tipo de mecanismo de algoritmo a utilizar.
Despliegue	Definir la plataforma a utilizar para lanzar el Blockchain
Entorno de Ejecución	Medio por el cual se ejecutan los recursos soportados para el Blockchain
Tipos de Nodos	Según la plataforma utilizadas los nodos pueden asumir diferentes roles un momento específico de una transacción
Soporte y Documentación	Plataforma de código abierto o cerrado y su nivel de instrumentación
Bifurcación de Plataforma origen.	Se refiere a que una plataforma puede dar origen a plataformas derivadas de esta, lo cual debe tomarse en cuenta al momento de escoger la plataforma a utilizar.
Tipo de Gobernanza	Se refiere a si es de carácter pública o privado

Para poder comprender de mejor manera la tecnología Blockchain es necesario conocer los componentes empleados dentro de un ambiente Blockchain, logrando entender con mayor detalle la cadena de eventos que ocurren al realizar transacciones mediante Blockchain. Para es necesario conocer el papel que los actores, servicios y procesos desempeñan al momento de ejecutarse las transacciones.

A continuación, describen las características técnicas de una Blockchain, específicamente sus componentes y las relaciones entre ellos. Como lo indica su nombre, una Blockchain como estructura de datos, es una secuencia de bloques la cual permite almacenar una lista completa de registros de transacciones. Utilizando una criptomoneda como ejemplo, y al igual que sucede en una gran cantidad de implementaciones, cada bloque contiene un encabezado en el cual se almacena el **hash** que identifica al bloque anterior de la cadena. Al primer bloque de la cadena comúnmente se le denomina **bloque génesis** y es el único que no contiene una referencia a un bloque anterior.

En la siguiente imagen se puede observar un ejemplo de estructura de bloques en donde cada uno contiene el hash que identifica al bloque de la cadena anterior, **una marca de tiempo**, un **campo nonce** utilizado en Bitcoin para el cálculo del hash del bloque y la secuencia de transacciones agregadas en el bloque actual. Es necesario aclarar que la estructura específica de cada bloque difiere según las diferentes implementaciones y los conceptos que en ellas se utilizan.

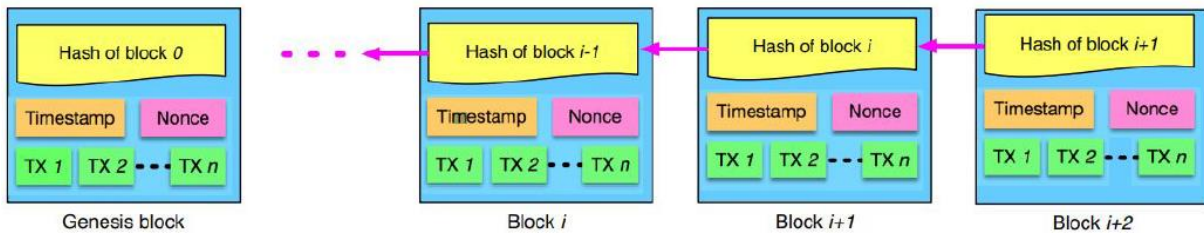


Ilustración 1 Ejemplo de Blockchain ilustrada en (10)

En el artículo “Cloud Customer Architecture for Blockchain” (34) se ilustra en alto nivel la estructura de una red Blockchain, la cual puede observarse en la siguiente imagen. En la imagen es posible identificar cinco componentes principales de la arquitectura: los usuarios (User), los nodos (Node), la cadena de bloques (ledger) y los mecanismos de seguridad (llave) y comunicación utilizados (enlaces).

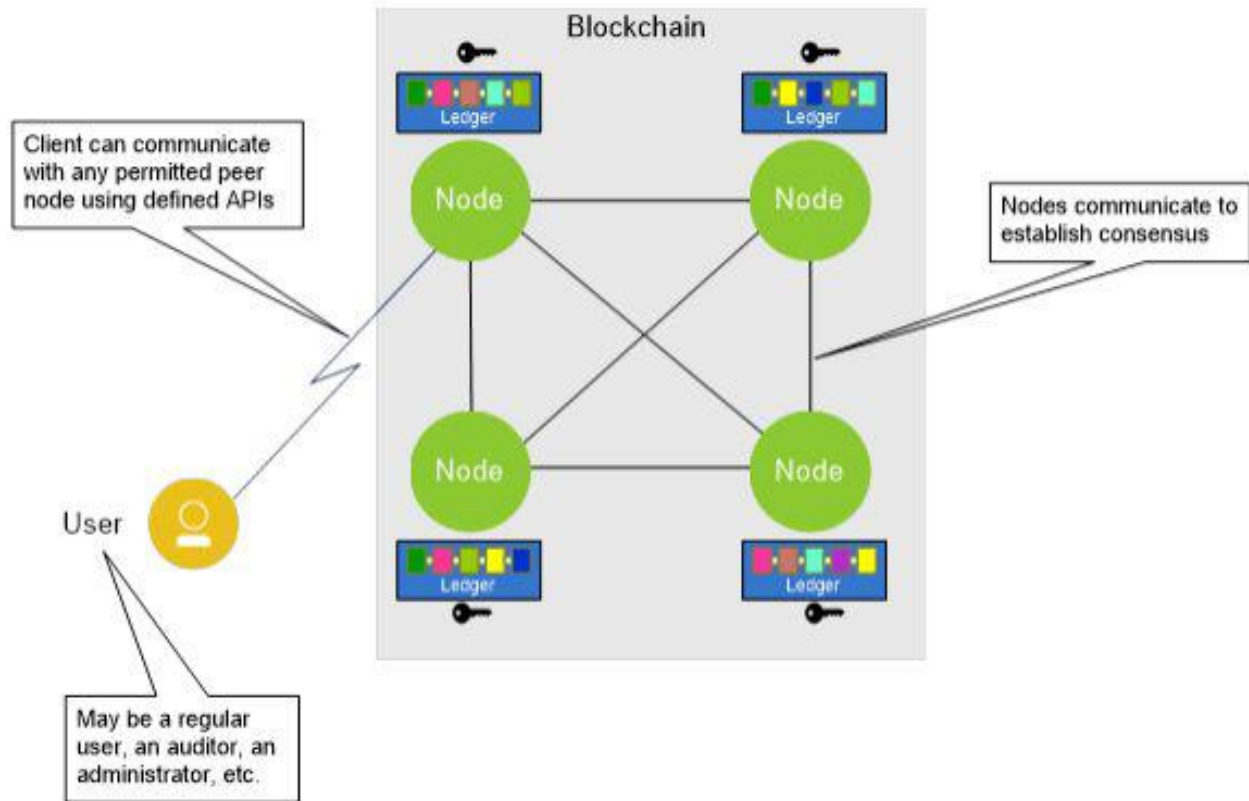


Ilustración 2 Vista en alto nivel de una red Blockchain (37)

La cadena de bloques es construida y mantenida en conjunto por los nodos de la red, los cuales almacenan la totalidad o porciones de la cadena localmente, dependiendo esto también de cada implementación particular. Los **usuarios** (individuos o agentes de software), realizan solicitudes de **transacciones**, típicamente utilizando APIs, para efectuar diferentes operaciones que el sistema se encuentra diseñado para proveer. Los **nodos**, se comunican entre sí para verificar la validez de las transacciones y determinar qué **bloques** son insertados en la cadena. Una vez que se efectúa una transacción y se registra en un bloque, esta nunca puede ser modificada o eliminada, garantizando la inmutabilidad. En relación a la seguridad, tanto de la información almacenada en la Blockchain, como en la comunicación entre nodos, se utiliza criptografía. Mediante la utilización de parejas de claves públicas y privadas se garantiza la integridad de los mensajes intercambiados entre nodos, así como también el hecho que determinadas operaciones sean efectuadas por entidades autorizadas.

En “A Reference Model for Blockchain-Based Distributed Ledger Technology” (35) de Andreas Ellervee, se propone un modelo de referencia que pretende asistir a analistas de negocio y sistemas, en el desarrollo de nuevas plataformas o implementaciones de la tecnología, haciendo hincapié en sus propiedades a nivel de negocio identificando los siguientes componentes: actores, roles, servicios, procesos y modelo de datos. El modelo de referencia propuesto por Andreas Ellervee resulta apropiado para la presentación de la arquitectura de una Blockchain para esta investigación ya que surge del análisis de plataformas existentes, construyendo un modelo con un alto grado de generalización.

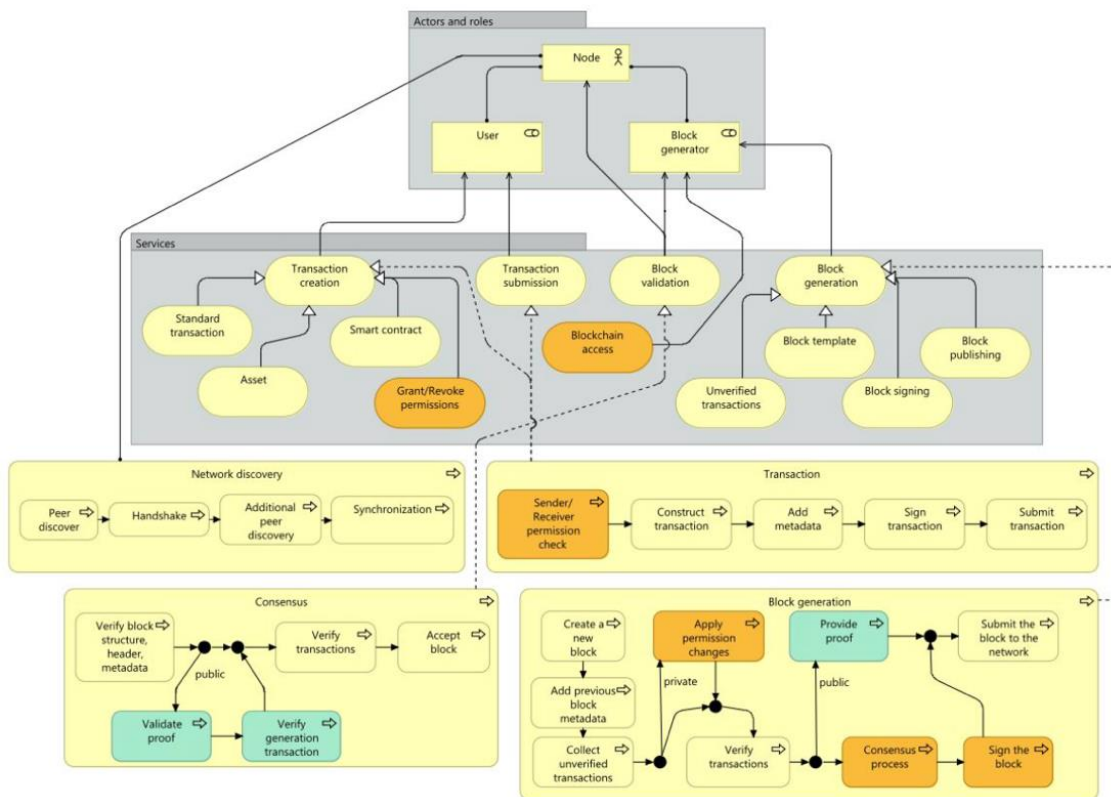


Ilustración 3 Modelo de referencia propuesto por Andreas Ellervee (38)

Actores. Desde una perspectiva de negocio se definen dos actores.

- **Usuarios:** quienes interactúan con la red de nodos realizando transacciones.

- **Generador de bloques:** responsable de la verificación y validación de transacciones, construcción de nuevos bloques y publicación de bloques en la red.

Servicios. Refiere a los recursos provistos por la red y se definen los siguientes:

- **Creación de transacciones:** utilizado para que los usuarios puedan agregar información a la Blockchain.
- **Envío de transacciones:** este servicio es utilizado para realizar el envío de las transacciones y la firma de las mismas.
- **Validación de bloques:** servicio utilizado por los nodos para validar y decidir qué bloques se insertan en la cadena.
- **Generación de bloques:** hace referencia al proceso de minería, en color naranja, se destacan servicios específicos utilizados en redes privadas.

Procesos: Se refiere a la serie de pasos que se ejecutan en este tipo de aplicaciones, en el modelo de referencia se proponen cuatro:

- **Descubrimiento de la red:** Permite a los nodos que ingresan a la red conectarse a los pares existentes y conocer la red.
- **Crear y enviar transacciones a la red:** Proceso de crear una transacción con sus metadatos, firmarla y enviarla a la red para su posterior validación.
- **Consenso:** hace referencia al mecanismo utilizado por los nodos para determinar qué bloques insertar en la cadena y el orden de los mismos.
- **Generación de bloques:** Refiere al proceso asociado al servicio de generación de bloques

Modelo de Datos. En el contexto de Blockchain típicamente refiere a un contenedor de los recursos, no necesariamente criptomonedas, de un usuario de la red condicionando su posibilidad de efectuar transacciones.

Este modelo organiza las diferentes prestaciones en función de la red en la cual se ubican: red pública, nube y red empresarial. Sin embargo, se menciona que cada uno de los componentes pueden ubicarse en las diferentes redes en función de las necesidades, así como también, si bien se recomienda la utilización de computación en la nube para dar soporte a la plataforma de Blockchain y sus servicios, este no es un requisito excluyente.

Seguridad y Privacidad de Blockchain

Según ISO/IEC 27002, la seguridad de la información es la preservación de la confidencialidad, integridad y la disponibilidad de la información. La integridad es una característica intrínseca de la tecnología Blockchain, por lo cual no aporta valor a la hora de decidir entre una plataforma u otra debido a que cualquier plataforma debería asegurar dicha característica. Las plataformas de Blockchain implementan diferentes mecanismos para garantizar la seguridad y por lo que al momento de seleccionar una plataforma se deben tener en cuenta los siguientes factores:

- **Mecanismo de Cifrado.** Se refiere a la forma de cifrar la información utilizado para la comunicación entre nodos. En algunos casos podría descartarse la clasificación según este mecanismo ya que es probable que todas las plataformas utilicen TLS.
- **Control Acceso Libro Mayor.** Se refiere a si existe un mecanismo que permita restringir el acceso al libro mayor, es decir, que no todos los nodos de la red tengan acceso a todas las transacciones de la Blockchain. Este control de acceso al libro mayor puede ser:
 - Obligatorio: la plataforma implementa un mecanismo de control de acceso al libro mayor y no provee de un mecanismo para no utilizarlo.
 - Opcional: la plataforma implementa un mecanismo de control de acceso al libro mayor y la utilización de dicho mecanismo es opcional.
 - No: la plataforma no implementa un mecanismo de control de acceso al libro mayor.

- **Consenso.** La clasificación definida en cuanto al consenso se define en función del mecanismo utilizado (es decir, el algoritmo) y si este es intercambiable, es decir si pueden utilizarse diferentes mecanismos en diferentes contextos dentro de la plataforma, entonces se dice que es un consenso intercambiable de lo contrario es un consenso fijo.
- **Despliegue.** Al construir una red de Blockchain las plataformas proveen diferentes mecanismos para realizar el despliegue de los nodos. Este punto permite brindar información acerca de las posibilidades y si los principales proveedores de infraestructura brindan entornos preconfigurados para trabajar con plataformas Blockchain. Las alternativas identificadas hasta el momento son:
 - Despliegue en la nube, es decir existen proveedores que brindan servidores preconfigurados con el software necesario.
 - Despliegue utilizando contenedores Docker u otros mecanismos, por ejemplo, como un servicio del sistema operativo.
- **Entorno de Ejecución.** Se refiere al entorno de ejecución de los nodos. A modo de ejemplo, la plataforma Ethereum implementó su propia máquina virtual denominada Ethereum Virtual Machine (EVM), en Corda los nodos ejecutan en una JVM con restricciones particulares, entre otros.
- **Tipos de Nodos.** Según la plataforma considerada, los nodos de la red pueden adquirir diferentes roles y ejecutar diferentes acciones. Cada plataforma define nombres específicos para los diferentes tipos de nodos. Entre los cuales se encuentran los siguientes:
 - Oráculo: Nodo que permite obtener información del “mundo exterior”, es decir, fuera de la red.

- Verificador: Nodo encargado de verificar las transacciones (que estén firmadas por los involucrados, que no ocurra doble gasto, que se cumplan las condiciones especificadas en contratos, etc.)
 - Portero: Nodo encargado de controlar el acceso a una Blockchain (verifica la identidad y asigna identificación a los nodos)
 - Ordenador: Nodo encargado de determinar el orden de las transacciones
 - Pares comunes: Nodos que se comunican con las aplicaciones y el resto de los nodos de la red.
- **Soporte y Documentación.** Se decide cuantificar el nivel de soporte y documentación provisto por la plataforma en función de si la plataforma es código abierto o no, si existe documentación técnica accesible en internet, si existe un whitepaper asociado y si se cuenta con una comunidad. Respecto a la comunidad, se considera que una plataforma cuenta con ella si existe un conjunto de personas que se encuentra utilizando la tecnología y mantienen una plataforma de intercambio accesible como puede ser Twitter, Slack, GitHub, entre otros.
 - **Bifurcación de plataforma origen.** Al estudiar las plataformas Blockchain es posible identificar que muchas de ellas se construyen a partir de implementaciones existentes de esta tecnología. Resulta de especial interés conocer si estas surgen como una bifurcación de alguna de las existentes y de esta manera conocer o tener una idea de los antecedentes de la misma.
 - **Tipo de Gobernanza:** Refiere a si la plataforma es gobernada de forma abierta (pública) o si es gobernada por una entidad u organización (privada)

4.1.3. SITUACIÓN ACTUAL, VENTAJAS Y DESVENTAJAS.

Objetivo 3: Definir la situación actual del Blockchain, ventajas y desventajas

Tabla 8 Variables de Entorno en el uso actual de Blockchain

Variables del Entorno Actual en el Uso de Blockchain	
Variable de Entorno	Descripción
Nivel de Adopción	Se refiere al nivel de adopción que actualmente posee la tecnología Blockchain en los distintos ámbitos en los que puede aplicarse.
Madurez Marco Jurídico	Se analiza el marco jurídico actual y como esta tiene incidencia en la adopción de la tecnología Blockchain.

Tabla 9 Ventajas Tecnología Blockchain

Ventajas Tecnología Blockchain	
Ventajas	Descripción
Durabilidad	Por su naturaleza las cadenas de bloques o Blockchain son más duraderas debido a que eliminan puntos de fallas de forma aislada sin afectar la red completa.
Transparencia	Por los detalles que genera cada una de las transacciones realizadas en Blockchain estas pueden ser rastreables hasta su origen.
Inmutabilidad	Los datos permanecen prácticamente sin modificaciones ya que para ello se necesita la validación de otros nodos lo cual lo hace la información confiable
Integridad del Proceso	La falta de intervención externa hace que los procesos se ejecuten de manera eficiente y sin alteraciones.

Tabla 10 Desventajas Tecnología Blockchain

Desventajas Tecnología Blockchain	
Desventajas	Descripción
Inyección de Código Externo	Se pueden crear vectores de ataque por errores humanos al momento de arreglar o mejorar funcionalidades a nivel de código fuente.
Peer-to-Peer	No se puede determinar responsables cuando ocurre un problema.
Escalabilidad	El número de transacciones utilizando Blockchain es muy reducido en comparación al número de transacciones en otros ámbitos.
Transparencia	Toda transacción es rastreable por lo que no existe el anonimato
Ataque del 51%	La concentración de poder de procesamiento en el minado de criptomonedas en una sola persona o grupo de personas asociadas entre sí, puede dar lugar a estafas o robo de criptomonedas a través del engaño en la cadena de bloques

Durante la investigación **con respecto al estado actual de la tecnología Blockchain**, se puede observar que muchas industrias lo están adoptando, pero al mismo tiempo se presentan desventajas que son simplemente un problema para que la adopción sea fácil para las entidades y para los usuarios, entre las desventajas podemos mencionar el hecho que determinadas operaciones sean efectuadas por entidades autorizadas; representando esto último una desventaja significativa con respecto a las transacciones tradicionales, las cuales al prescindir de este tipo tecnología pueden ser aplicadas en grandes escalas en tiempos reducidos, para igualar estos tiempos y resultados los entornos Blockchain deben con una infraestructura robusta desplegada a gran escala que permita realizar transacciones a nivel con la complejidad que el Blockchain demanda. Esto significaría modernizar los equipos servidores actuales dentro de las instituciones financieras a corto plazo resultando en elevados costos de

implementación sin contar las horas de capacitación requeridas para el personal involucrado.

Con base a los documentos legales mencionados en este documento se puede constatar que no existen mecanismos que regulen los usos de esta tecnología. La falta de mecanismos legales que regulen dicha tecnología implica un gran obstáculo para su adopción e implementación. Lo cual conlleva a la oportunidad de utilizar el Blockchain para realizar delitos de lavado de activos y otras acciones ilícitas. Para tener una perspectiva las ventajas y desventajas del uso de Blockchain basta con comparar como se realizan las transacciones bancarias en forma tradicional contra las transacciones que utilizar esta nueva tecnología, teniendo como principales ventajas: durabilidad, transparencia, inmutabilidad e integridad del proceso, que en resumen garantizan que la transacción se hecha de forma segura y la información sea accedida únicamente por las partes interesadas. Por otra parte, las desventajas del uso de esta tecnología radican en: la incapacidad de determinar el nodo responsable de un problema, la escalabilidad debido a la limitante de plataformas que brindan el servicio, y la transparencia lo cual se refiere a que toda transacción puede ser rastreada y ser visible contradiciendo el espíritu del anonimato de Blockchain.

VENTAJAS.

La tecnología posiblemente más importante de la última década que está cambiando poco a poco el mundo, y entre sus ventajas se pueden mencionar:

Durabilidad. Las redes descentralizadas eliminan puntos únicos de falla en lugar de sistemas centralizados. Esta distribución del riesgo entre sus nodos hace que las cadenas de bloques sean mucho más duraderas que los sistemas centralizados y que sean más adecuadas para evitar los ataques maliciosos.

Transparencia. Cada nodo en la red mantiene una copia idéntica de una cadena de bloques, lo que permite la auditoría e inspección de los conjuntos de datos en tiempo real. Este nivel de transparencia hace que las actividades y operaciones de la red sean muy visibles, reduciendo así la necesidad de confianza

Inmutabilidad. Los datos que se almacenan en un Blockchain público distribuido son prácticamente inmutables debido a la necesidad de validación por parte de otros nodos y rastreabilidad de cambios. Esto permite a los usuarios operar con el mayor grado de confianza, ya que la cadena de datos es exacta e inalterable.

Integridad del Proceso. los protocolos distribuidos de código abierto se ejecutan por naturaleza exactamente como están escritos en el código. Los usuarios pueden estar seguros que las acciones descritas en el protocolo se ejecutan de forma correcta y oportuna sin necesidad de intervención humana.

DESVENTAJAS.

Como toda tecnología emergente el Blockchain tiene un gran potencial y por su naturaleza criptográfica y su forma de funcionar, pero también posee desventajas inherentes a lo que es la tecnología como tal. La complejidad que caracteriza al Blockchain, dificulta en algunos casos la adopción de la misma o lleva a la elaboración de conceptos erróneos, motiva el planteo de soluciones que sugieren la utilización de Blockchain en escenarios en donde su aplicación no resulta justificada.

Inyección de Código Externo. Hace referencia a un posible código malicioso externo no controlado. Este tipo de debilidad suele aparecer cuando es necesario añadir una funcionalidad o corregir un error por medio de esa “referencia” y se abren vectores de ataque que pueden afectar a la integridad de la cadena de bloques, intencionadamente o por un error humano. Aunque en Blockchains públicas (Bitcoin, Ethereum, etc.)

Peer-to-Peer. Los nodos no son identificables y esto puede derivar en fraudes, virus o contenidos erróneos. Cuando ocurre un problema no se puede determinar al responsable.

Escalabilidad. El número posible de transacciones de pago es reducido en comparación con la escala de transacción dentro de la economía real.

Transparencia. Dado que los detalles de la transacción se revelan, todas las transacciones se pueden rastrear. La garantía perfecta de pseudo-anonimato puede ser difícil, y la re-identificación mediante la combinación es posible.

Ataque del 51%. Se trata de una amenaza a la que cualquier Blockchain es susceptible de ser víctima, debido a que la mayoría están basadas en cadenas de bloques que utilizan protocolos de prueba de trabajo para verificar las transacciones. Un protocolo de Blockchain es un conjunto de reglas que determinan cómo las computadoras conectadas a una red deberán verificar nuevas transacciones y añadirlas a la base de datos. En el proceso de verificación (conocido como minería) los distintos nodos de una red consumen grandes cantidades de poder de procesamiento para demostrarse que son lo suficientemente confiables para añadir información sobre una nueva transacción a la base de datos. En este sentido, “un minero que de alguna manera obtiene control de una mayoría del poder de minería de una red puede engañar a otros usuarios enviándoles pagos y luego crear una versión alternativa de la Blockchain, denominada fork, en la cual el pago nunca ocurrió, explica el artículo de Technology Review. Por lo tanto, un atacante que controle el mayor porcentaje del poder de procesamiento puede hacer que el fork sea la versión de más autoridad de la cadena y proceder a gastar la misma criptomoneda nuevamente” Llevar adelante un ataque del 51% contra las criptomonedas más populares puede resultar demasiado costoso por el poder de cómputo que requiere y el costo de conseguirlo, lo que llevó a que en 2018 los cibercriminales realizaran ataques de este tipo dirigidos hacia criptomonedas de menor renombre y que exigen menor poder de cómputo; logrando robar hasta 120 millones de dólares en total.

5. CAPÍTULO 5

5.1. PROPUESTA DE USO

La aplicación de este ejemplo utiliza Blockchain para llevar un registro de diferentes participantes de la red. La red desplegada se constituye de tres nodos: A, B y C. Donde A es el nodo prestador de servicios de salud, B es el nodo que representa al Ministerio de Salud y C es el nodo que representa al Instituto Salvadoreño del Seguro Social (ISSS), entidad a la cual los distintos prestadores de servicio y el Ministerio de Salud solicitan acceso a las historias clínicas electrónicas (HCE).

La interacción del usuario de la aplicación con la red Blockchain se realiza a través de una interfaz web en la cual se realizan las solicitudes de registro y consultas de HCE. El escenario propuesto es utilizar Blockchain como un registro de auditoría respecto al acceso a las historias clínicas electrónicas por parte de los diferentes actores del ecosistema.

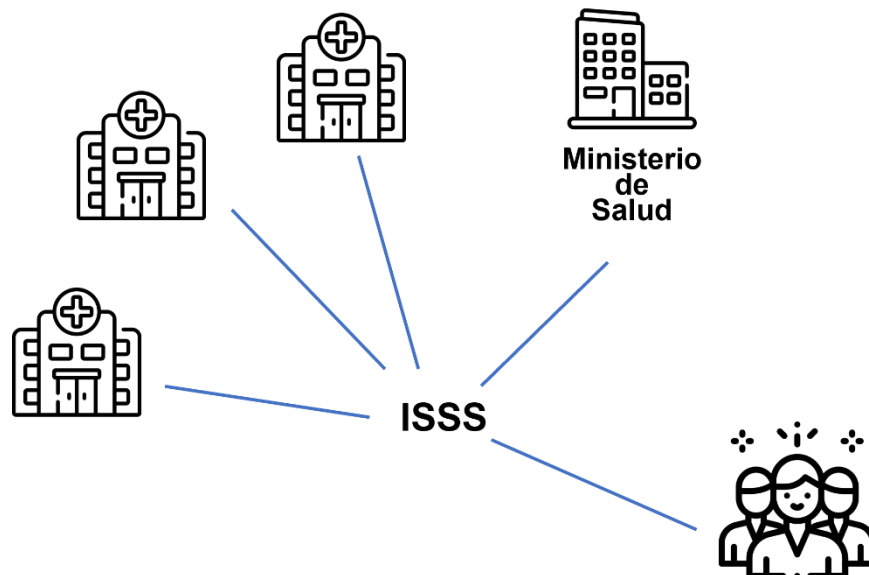


Ilustración 4 Imagen de Referencia

El objetivo de utilizar una Blockchain en este escenario es brindar un mecanismo que garantice al usuario del ecosistema, es decir al paciente, el acceso autorizado a su historia clínica. Para ello se propone que cada vez que un prestador o el Ministerio de Salud soliciten al

ISSS el acceso a una HCE, se invoque a un servicio que registre en Blockchain el acceso a su HCE (registrando el DUI del paciente y un identificador para el diagnóstico médico del paciente que solicita obtener de su historia clínica). Como fue mencionado, el acceso se restringe a los participantes de una transacción, de este modo los prestadores de salud conocen únicamente sus solicitudes y no es posible que otros prestadores las conozcan (garantizando la privacidad de las mismas); pero siendo todas estas transacciones accesibles para el Instituto Salvadoreño del Seguro Social (ISSS).

Se propone la implementación de una aplicación web para que los pacientes puedan verificar los accesos a sus HCE, lo cual se resuelve realizando una consulta sobre el Blockchain, verificando los siguientes datos, el DUI del paciente, la validación que el identificador del diagnóstico médico sea mayor que cero y que uno de los participantes sea el Instituto Salvadoreño del Seguro Social.

Por último, en la API utilizada por la aplicación web, de modo que el método invocado al querer ingresar un registro en el Blockchain reciba los parámetros: código identificador del diagnóstico médico y DUI del paciente. Con este ejemplo se da a conocer uno de tantos usos de una plataforma Blockchain para un futuro cercano.

6. CAPÍTULO 6

6.1. CONCLUSIONES Y RECOMENDACIONES

6.1.1. CONCLUSIONES

En relación con la problemática podemos decir que a pesar de que se tiene por sentado que Blockchain está ligado a monedas y tokens digitales, sin embargo, esta tecnología no se limita a soluciones financieras, también puede ser una alternativa de solución para otros ámbitos tales como cadenas de suministros del sector comercio, así como también para el sector salud por el tipo de información sensible que se maneja puede ser de mucha utilidad para guardar historiales médicos.

Con relación al objetivo número dos se destacan los componentes principales que conforman la cadena de bloques entre los cuales se destacan: las funciones Hash, el Bloque génesis, el Campo nonce, los Nodos, las Transacciones, los Actores, los Procesos y los Servicios.

En relación con el tercer objetivo se puede decir que la situación en el contexto nacional e internacional de Blockchain muestra que es una tecnología utilizada en su mayoría como un libro mayor de transacciones atados a criptoactivos, en su mayoría Bitcoin, Ethereum, Dogecoin entre otros.

A su vez se puede concluir que actualmente no existe un marco regulatorio o normativo especializado en Blockchain que ampare una adopción e implementación amigable en el ámbito nacional, ya que las leyes actuales no contemplan todo el espectro correspondiente a la tecnología Blockchain como tal.

Se pueden resaltar las bondades que esta tecnología posee de forma inherente con respecto a la seguridad, siendo estas lo que más llama la atención y por lo que muchos ámbitos

entre ellos financieros, comerciales, salud, logística entre otros buscan migrar sus procesos adoptándola como una solución a los problemas actuales.

6.1.2. RECOMENDACIONES

Se recomienda que el país tome una política más completa en cuanto al tema de Blockchain en el ámbito legal y para dar seguridad jurídica al uso de esta tecnología, evitando posibles delitos de lavado de dinero, blanqueamiento de activos y otro tipo actos ilegales que se pueden llevar a cabo al tener leyes poco eficientes.

Para el ámbito educativo y profesional se recomienda que los centros de estudio incluyan programas para capacitar y formar profesionales dentro de la rama de Blockchain ya que se observa que uno de los problemas para la implementación y administración de esta tecnología es la falta de profesionales con formación específica en esta área.

Respecto a la infraestructura necesaria para soportar el Blockchain se recomienda evaluar opciones en la nube que permitan una respuesta inmediata ante una demanda cambiante de las tecnologías Blockchain, garantizando soluciones vigentes a largo plazo.

7. REFERENCIAS BIBLIOGRÁFICAS

1. **Abeyratne, Saveen A. y Monfared, Radmehr P.** *BLOCKCHAIN READY MANUFACTURING SUPPLY CHAIN*. 2016.
2. **Forbes Insights.** Forbes. [En línea] 2021. [Citado el: 12 de Marzo de 2022.] https://www.forbes.com/forbesinsights/sap_transactions/index.html.
3. **Oh, J y Shong, I.** *A case study on business model innovations using Blockchain: focusing on financial institutions*. 2018.
4. **Viriyasitavat, W y Hoonsopon, D.** *Blockchain characteristics and consensus in modern business processes*. 2018.
5. **Cermeño, Javier Sebastian.** *Blockchain in financial services: Regulatory landscape and future challenges for its commercial application*. s.l. : BBVA Research, 2016.
6. **Asamblea Legislativa de la Republica de El Salvador.** Ley Bitcoin. San Salvador : s.n., 2021.
7. **Banco Central de Reserva de El Salvador.** NORMAS TÉCNICAS PARA FACILITAR LA PARTICIPACIÓN DE ENTIDADES FINANCIERAS EN ECOSISTEMA BITCOIN. San Salvador : s.n., 2021.
8. —. LINEAMIENTOS PARA LA AUTORIZACIÓN DEL FUNCIONAMIENTO DE LA PLATAFORMA DE LA BILLETERA DIGITAL PARA BITCOIN Y DÓLARES. San Salvador : s.n., 2021.
9. **Ekblaw, Ariel.** *A Case Study for Blockchain in Healthcare: “MedRec” prototype for electronic health records and medical research data*. s.l. : MIT Media Lab, 2016.
10. **DokChain.** DokChain PokitDok. [En línea] <https://pokitdok.com/dokchain/>.
11. **Smith, Bryan.** DOKCHAIN: INTELLIGENT AUTOMATION IN HEALTHCARE TRANSACTION PROCESSING. 2017.
12. **Roberts, Jeff John.** *Are You Eating Sustainable Fish? Blockchain May Provide the Answer*. s.l. : Fortune, 2018.
13. **IBM.** IBM Announces Major Blockchain Collaboration with Dole, Driscoll's, Golden State Foods, Kroger, McCormick and Company, McLane Company, Nestlé, Tyson Foods, Unilever and Walmart to Address Food Safety Worldwide. [En línea] 22 de Agosto de 2017. <https://newsroom.ibm.com/2017-08-22-IBM-Announces-Major-Blockchain-Collaboration-with-Dole-Driscolls-Golden-State-Foods-Kroger-McCormick-and-Company-McLane-Company-Nestle-Tyson-Foods-Unilever-and-Walmart-to-Address-Food-Safety-Worldwide>.
14. **IBM Consulting.** *IBM Blockchain and SAP IoT Solution for the Pharmaceutical Cold Chain*. 2017.
15. **Insurwave.** [En línea] <https://insurwave.com/>.
16. **Newswire.** World's first blockchain platform for marine insurance now in commercial use. [En línea] 2018. <https://markets.businessinsider.com/news/stocks/world-s-first-blockchain-platform-for-marine-insurance-now-in-commercial-use-1025259012>.

17. **Ernst and Young.** Better-working insurance: moving blockchain from concept to reality. [En línea] 2017. https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/insurance/insurance-pdfs/ey-marine-blockchain-pov.pdf.

18. **TrustChain.** TrustChain. [En línea] <https://www.trustchainjewelry.com/>.

19. *Towards an Ontology-Driven Blockchain Design for Supply Chain Provenance.* **Kim, Henry M y Laskowski, Marek.** s.l. : SSRN Electronic Journal, 2016.

20. **Novo, Oscar.** *Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT.* s.l. : IEEE, 2018.

21. **Koetsier, John.** Programming as Art: How Blockchain Can Help Artists (And Save Art). [En línea] 23 de Mayo de 2018. <https://www.inc.com/john-koetsier/programming-as-art-how-blockchain-can-help-artists-and-save-art.html>.

22. **Rodrigues, Viviane y Urban, John.** This Startup Is Using Blockchain to Fight Art Forgers. *Bloomberg.* [En línea] 23 de Marzo de 2018. <https://www.bloomberg.com/news/articles/2018-03-23/art-forgers-find-a-new-enemy-in-verisart-s-blockchain-startup>.

23. **Rossow, Andrew.** Why Does The Art Community Need Blockchain On Its Palette? *Forbes.* [En línea] 7 de Abril de 2018. <https://www.forbes.com/sites/andrewrossow/2018/04/07/why-does-the-art-community-need-blockchain-on-its-palette/?sh=892e5a24044c>.

24. **Verisart y Mannion, Shelley.** Why Should I Use It? [En línea] <https://help.verisart.com/en/articles/4568851-why-should-i-use-verisart#:~:text=Unique%20certification%20of%20authenticity%20for,your%20own%20style%20and%20branding>.

25. **Ujo Music.** Ujo Music. [En línea] <https://blog.ujomusic.com/>.

26. **IBM Blockchain Pulse.** Challenge Accepted: Your Chance to Make the World Better with Blockchain. [En línea] Mayo de 2018. <https://www.ibm.com/blogs/blockchain/2018/05/challenge-accepted-chance-make-world-better-blockchain/>.

27. **IBM Corporation.** Identity Now - Building a Digital Identity Ecosystem on Blockchain with SecureKey in the Banking Industry. [En línea] <https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=BKW03040USEN>.

28. **ETHLend.** [En línea] <https://ethlend.io/es>.

29. **Weifund.** [En línea] <http://weifund.io/>.

30. **Wikipedia, La Enciclopedia Libre.** Democracia Liquida. [En línea] [Citado el: 16 de Junio de 2022.] https://es.wikipedia.org/wiki/Democracia_L%C3%ADquida.

31. **Dash.** Gobernanza de Dash. [En línea] <https://docs.dash.org/es/stable/governance/index.html>.

32. **Bingsheng, Zhang, Oliykyov, Roman y Balogun, Hamed.** *A Treasury System for Cryptocurrencies: Enabling Better Collaborative Intelligence.*

33. **Alketbi, Ahmed.** *Blockchain for government services — Use cases, security benefits and challenges*. s.l. : IEEE, 2018.
34. **Cloud Standards Customer Council.** Cloud Customer Architecture for Blockchain. [En línea] 2017. <https://www.omg.org/cloud/deliverables/CSCC-Cloud-Customer-Architecture-for-Blockchain.pdf>.
35. **Ellervee, Andreas.** A Reference Model for Blockchain-Based Distributed Ledger Technology. [En línea] https://comserv.cs.ut.ee/home/files/ellervee_softwareengineering_2017.pdf?study=ATILoputoo&reference=77BCAF0F09164BE4DB593978F449D0B493FFE7BA.
36. **Viant.** [En línea] <https://viant.io>.
37. **Yan, Chen.** *Blockchain tokens and the potential*. 2018.
38. **Sunmola, Funlade T. y Apeji, Uje D.** *Blockchain Characteristics for Sustainable Supply Chain*. 2020.

8. ANEXOS

Anexo 1

Tabla 11 Anexo 1 - Criterios de Adopción Blockchain

Tabla de criterios de entornos para adopción de Blockchain		
No	Criterio	Descripción

Anexo 2

Tabla 12 Anexo 2 - Entornos de Uso Blockchain

Tabla de entornos de uso Blockchain	
Entornos	Descripción

Anexo 3

Tabla 13 Anexo 3 - Componentes del Blockchain

Componentes del Blockchain	
Componente	Descripción

Anexo 4

Tabla 14 Anexo 4 - Seguridad y Privacidad del Blockchain

Seguridad y Privacidad del Blockchain	
Mecanismo de Seguridad	Descripción

Anexo 5

Tabla 15 Anexo 5 - Variables de entorno actual en el uso de Blockchain

Variables del Entorno Actual en el Uso de Blockchain	
Variable de Entorno	Descripción

Anexo 6

Tabla 16 Anexo 6 - Ventajas uso Blockchain

Ventajas Tecnología Blockchain	
Ventajas	Descripción

Anexo 7

Tabla 17 Anexo 7 - Desventajas uso Blockchain

Desventajas Tecnología Blockchain	
Desventajas	Descripción