

2018

ANÁLISIS DE LA TECNOLOGÍA BLOCKCHAIN, SU ENTORNO Y SU IMPACTO EN MODELOS DE NEGOCIOS

ALVAREZ ROJAS, LUIS RODRIGO

<https://hdl.handle.net/11673/47346>

Repositorio Digital USM, UNIVERSIDAD TECNICA FEDERICO SANTA MARIA



ESCUELA DE NEGOCIOS
DEPARTAMENTO DE INGENIERÍA COMERCIAL
UNIVERSIDAD TÉCNICA
FEDERICO SANTA MARÍA

UNIVERSIDAD TÉCNICA FEDERICO SANTA MARÍA
Escuela de Negocios Departamento de Ingeniería Comercial
MBA, Magíster en Gestión Empresarial

ANÁLISIS DE LA TECNOLOGÍA BLOCKCHAIN, SU ENTORNO Y SU IMPACTO EN MODELOS DE NEGOCIOS

Tesina de Grado presentada por

Luis Rodrigo Álvarez Rojas

Como requisito para optar al grado de
MBA, Magíster en Gestión Empresarial

Guía de Tesina Dr. Pablo Isla Madariaga

Noviembre de 2018

TITULO DE TESINA: **“ANÁLISIS DE LA TECNOLOGÍA
BLOCKCHAIN, SU ENTORNO Y SU IMPACTO
EN MODELOS DE NEGOCIOS”**

AUTOR: **Luis Rodrigo Álvarez Rojas**

TRABAJO DE TESINA, presentando en cumplimiento parcial de los requisitos para el Grado de MBA, Magíster en Gestión Empresarial de la Universidad Técnica Federico Santa María.

OBSERVACIONES:

COMISIÓN DE TESINA: Dr. Pablo Isla M.
 Dr. Zócimo Campos J.
 Mg. José Miguel González P.

Santiago, Noviembre 2018

Todo el contenido, análisis, conclusiones y opiniones vertidas en este estudio son de mi exclusiva responsabilidad.

Nombre: Luis Rodrigo Álvarez Rojas.

Fecha: 27 de Noviembre de 2018.

Resumen y Conclusiones

Blockchain es un libro mayor distribuido que permite el registro de información, valor y activos en cualquiera de sus formas sin la ayuda de intermediarios, es considerada una de las tecnologías más innovadoras del último tiempo con la capacidad de modificar sistemas transaccionales otorgando seguridad, transparencia, descentralización y colaboración mientras concede poder a los usuarios, además posee la capacidad de mejorar procesos y reducir los costos de las transacciones. La tecnología blockchain posee el potencial para ser utilizada en una gran cantidad de industrias, como la financiera, cadena de suministro, legal, social, salud y sustentabilidad, por lo tanto es importante entender como impacta y beneficia a las empresas y sus modelos de negocios. Sin embargo la tecnología blockchain solo puede mostrar todo su potencial funcionando en red, por lo que se debe comprender la totalidad de su ecosistema y cuál es el valor que agrega cada uno de sus participantes.

El objetivo de este estudio es conocer en detalle el entorno de negocios de la Tecnología Blockchain, sus usos potenciales, impactos y beneficios para los modelos de negocios. De esta manera es importante conocer el estado actual de la tecnología, características, oportunidades ventajas y limitaciones, así como la identificación de áreas de negocios que serán impactadas mediante el uso de modelos de análisis estratégicos. Para el desarrollo del estudio se utiliza el trabajo realizado por Riasanow & Burckhardt (2018) para comprender el desarrollo el ecosistema blockchain y el modelo de negocios Canvas propuesto por Osterwalder & Pigneur (2010) para analizar a sus actores y potenciales impactos y oportunidades de negocios.

Utilizando el modelo de negocios Canvas se analizo a actores relevantes del ecosistema blockchain, encontrando que las empresas que poseen un mayor desarrollo y adopcion de la tecnologia correspondene al sistema financiero,

haciendo usos de blockchain consorcio para la mejora de sus procesos y reduccion de costos. Pero se debe tener presente que el verdadero potencial de la tecnología se puede apreciar en una red mayor y para ello es necesaria una rápida adopción, la generación de aplicaciones públicas descentralizadas apoyando el desarrollo de la infraestructura en un aspecto económico, empresarial y social. De esta manera son las empresas que basan sus modelos de negocio en el registro e intercambio de información y valor mediante cualquier clase de activos las que poseen un mayor riesgo de ser impactadas económica y financieramente por la tecnología blockchain, por medio de las aplicaciones descentralizadas que buscan el beneficio de todos sus miembros. Este tipo de empresas deben buscar formas de reducir las amenazas de la tecnología ya sea incorporándola o ajustando sus modelos de negocio.

Tabla de contenido

1. Introducción.....	11
2. Definición y Justificación del Tema	12
3. Objetivos	12
3.1. Objetivo General.....	12
3.2. Objetivo Especifico	12
4. Alcance del Estudio.....	13
5. Metodología de Trabajo	13
6. Estado del Arte.....	14
6.1. Antecedentes del Estado del Arte.....	14
6.2. Blockchain	16
6.3. Tipos de Blockchain.....	18
6.4. ¿Por qué es tan innovador?.....	21
6.4.1. Ventajas y Desventajas.....	23
6.5. Entorno Blockchain	25
6.5.1. Blockchain 1.0.....	26
6.5.2. Blockchain 2.0.....	27
6.5.3. Blockchain 3.0.....	28
6.6. La seguridad de Blockchain.....	29
6.6.1. El problema del 51%	29
6.6.2. Doble Gasto.....	29
6.6.3. Claves Privadas.....	30
7. Aplicaciones Blockchain.....	31
7.1. Escenarios integrados de IoT y Blockchain	32
7.2. Blockchain e Instituciones Financieras	33
7.3. Contratos inteligentes	35
7.4. Aplicaciones Sociales	36
7.5. Aplicaciones Legales	36
7.6. Cadena de Suministro	37

7.7.	Sustentabilidad	39
7.8.	Otras Aplicaciones	40
8.	Consideraciones Legales	41
9.	Marco Teórico del Estado del Arte	42
9.1.	Conceptos Claves.....	42
9.1.1.	Red Peer-to-Peer	42
9.1.2.	Encriptación de Clave Pública.....	42
9.1.3.	Algoritmo de Consenso	43
9.1.4.	Los Mineros.....	45
9.1.5.	Transacción.....	46
9.1.6.	Bloque	47
9.2.	Funcionamiento de la Blockchain	49
9.3.	Aplicaciones Descentralizadas Dapps	52
9.3.1.	DAO/DAC.....	54
9.3.2.	DAS.....	55
9.3.3.	Lanzamiento de una DApp.....	56
9.4.	Modelos de Negocio	57
9.5.	Valor estratégico y Ecosistema Blockchain	62
10.	Desarrollo del Tema.....	64
10.1.	Análisis Ecosistema Blockchain	64
10.1.1.	Consumidores	65
10.1.2.	Proveedores de Infraestructura Blockchain.....	65
10.1.3.	Proveedores de Plataforma Blockchain	69
10.1.4.	Proveedores de Aplicaciones Blockchain.....	71
10.1.5.	Proveedores de Plataforma Comunitaria Basadas en Tokens.....	74
10.1.6.	Minería	76
10.1.7.	Proveedores de Equipos y Soluciones Mineras	78
10.1.8.	Proveedores de Servicios Auxiliares	80
10.1.9.	Alianzas Blockchain	81
10.1.10.	Comunidad Blockchain	82

10.1.11. Servicios de Asesoramiento Blockchain	83
10.2. Modelo Ecosistema Blockchain	84
Conclusiones	89
11. Bibliografía	91

Índice de Tablas

Tabla 1. Capitalización de las principales criptomonedas. Fuente: Investing.com	66
---	----

Índice de Cuadros

Cuadro N°1. Características según tipo de blockchain. Fuente: Oh & Shong (2017).	20
Cuadro N°2. Características de Blockchain. Fuente Oh & Shong (2017).	24
Cuadro N°3. Aplicaciones IoT y Blockchain. Fuente: Reyna & Martín (2018)...	33
Cuadro N°4. Análisis modelo de negocio de proveedores de infraestructura blockchain.	68
Cuadro N°5. Análisis modelo de negocio proveedores de plataforma blockchain.	70
Cuadro N°6. Análisis de modelo de negocio de proveedores de aplicaciones blockchain.	73
Cuadro N°7. Análisis de modelo de negocio de las Mining Pool.	78

Índice de Gráficos

Gráficos N°1. Distribución de los principales Mining Pool de Bitcoin.	76
Gráficos N°2. Distribución de los principales Mining Pool de Ethereum.	77

Índices de Ilustraciones

Ilustración N°1. Funcionamiento de blockchain. Fuente: miethereum.com.	50
Ilustración N°2. Diagrama verificación de transacciones.	51
Ilustración N°3. Modelo de Negocios Canvas. Fuente: Macías (2012)	60
Ilustración N°4. Modelo Ecosistema Blockchain.	84

1. Introducción

El ritmo de la innovación tecnológica y de los negocios se ha acelerado durante las últimas décadas, dificultando la elaboración de modelos de negocios que mantengan una rentabilidad sostenida en el tiempo. En especial, Internet permite la creación de nuevos modelos de negocios con un alcance global instantáneo (Teece & Linden, 2017). Sin embargo internet carece en si misma de medios de pago, estructuras corporativas y formas de asociación que invalidan la separación del mundo digital del real (Lérida & Pérez, 2016). Blockchain es un libro mayor distribuido para garantizar seguridad y facilidad de acceso a nivel global, por lo que permite realizar transacciones de información o valor sin la necesidad de un tercero de confianza como el banco o el gobierno. De esta manera Blockchain trae una nueva web realizando una transición desde el internet de la información al internet del valor y se considera que tiene el potencial disruptivo para modificar los procesos y modelos de negocios.

A lo largo del tiempo las revoluciones tecnológicas han tenido un impacto positivo en el desarrollo, crecimiento e innovación tanto en el ámbito público como el privado, generando cambio en distintas industrias entregando nuevos productos, formas de comercialización y modificación de la forma en que las empresas generan valor para el mercado. No obstante las anteriores revoluciones se podrían diferenciar en la forma en la que se entrega y captura valor para los clientes, en este sentido blockchain con sus propiedades que le permiten no depender de un tercero de confianza promete beneficios para la comunidad, motivando el interés por la colaboración.

Las posibilidades y oportunidades que otorga la tecnología blockchain son diversas con una variedad de aplicaciones en distintas industrias que otorgan mejoras de procesos y transformaciones en la forma que se relacionan empresas y clientes. Estas características y utilidades han despertado el interés

por analizar la tecnología, su ecosistema, impacto y beneficios para las empresas, con el fin de aportar al conocimiento tanto académico como empresarial.

2. Definición y Justificación del Tema

La tecnología Blockchain ha experimentando un auge importante durante los últimos años. De la misma manera que internet cambió para siempre los modelos de negocio de industrias y empresas centenarias, blockchain o «cadena de bloques» está dando lugar, desde su aparición en 2009, a un nuevo patrón económico basado en la descentralización de la confianza, en donde todos podremos intercambiar bienes y servicios sin necesidad de terceros. Esto implica un avance sin parangón que revolucionara la manera en la que organizamos nuestra vida digital. De hecho, no en vano se dice que hemos pasado del internet de la información al internet del valor (Preukschat, 2017). La tecnología blockchain se considera la invención más significativa después de Internet (Efanov & Roschin, 2018).

3. Objetivos

3.1. Objetivo General

Conocer en detalle el entorno de negocios de la Tecnología Blockchain, sus usos potenciales, repercusión y beneficios para los modelos negocios.

3.2. Objetivo Especifico

- Identificar el estado actual de la Tecnología Blockchain, potenciales oportunidades, principales características, ventajas y limitaciones.

- Identificar modelos de análisis a utilizar para entender el desarrollo e impacto generado por la Tecnología Blockchain.
- Identificar áreas de negocios que serán impactadas por la tecnología mediante modelos de análisis estratégico.

4. Alcance del Estudio

El alcance del estudio contempla investigar el entorno de la tecnología Blockchain, su valor estratégico, potenciales aplicaciones de la tecnología distinto al sector de las criptomonedas. Entender cuáles son las industrias en las que se presentara un mayor impacto y como afectara a los modelos de negocio, de esta manera entender sus beneficios y áreas en las que se puede innovar utilizando esta tecnología como herramienta.

5. Metodología de Trabajo

La metodología utilizada consta de búsqueda de información de paper, revistas, análisis de aplicaciones actuales y páginas web especializadas para entender su funcionamiento, el nivel de desarrollo obtenido en la actualidad y cuáles son sus principales aplicaciones. Además, se emplean análisis de modelos estratégicos acordados para analizar el atractivo de las industrias en la adopción de la tecnología y así determinar a través de modelos de análisis de negocio cuáles son las industrias en que tendrá mayor incidencia.

6. Estado del Arte

Históricamente revoluciones tecnológicas han tenido poco impacto en los sistemas jerárquicos piramidales de las organizaciones y los gobiernos, pero la era de la información actual se cree que conduce a una sociedad motivada por el interés de la colaboración más que la ganancia individual. Esto podría llevar a la instalación de comunidades distribuidas y de consenso, independiente de intermediarios organizados jerárquicamente.

6.1. Antecedentes del Estado del Arte

La tecnología Blockchain es una innovación revolucionaria con la capacidad de transformar muchos sistemas tradicionales existentes en sistemas más seguros, distribuidos, transparentes y colaborativos, mientras que empodera a sus usuarios (Abeyratne & Monfared, 2016). La tecnología Blockchain fue noticia por primera vez como base para nuevos tipos de transacciones financieras, comenzando con Bitcoin en 2009. Para el 2020, la red de servicios profesionales 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 (Forbes, 2016).

Blockchain se ha convertido en una nueva frontera de capitales de riesgo que ha atraído la atención de bancos, gobiernos y otras corporaciones comerciales. 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 red (Zhao, Fan, & Yan, 2016). La tecnología blockchain que

sustenta a monedas digitales como el Bitcoin, podría tener consecuencias de largo alcance para todos los aspectos de la sociedad moderna. La tecnología Blockchain es esencialmente una base de datos de activos que se pueden compartir a través de una red de múltiples sitios, geografías o instituciones. Además Blockchain tiene la capacidad de ejecutar scripts autónomos. Este es el concepto de contrato inteligente; código controlado por datos que pueden representar una aplicación lógica verificable y ayuda a automatizar un conjunto de reglas del sistema (Huckle, Bhattacharya, White, & Beloff, 2016).

Para abordar los problemas de la adopción de blockchain en un entorno empresarial, son tres los niveles de estudios que pueden ser llevados a cabo por investigadores, incluidos los conceptuales, prescriptivos, y niveles descriptivos. Actualmente, la investigación comercial en blockchain se encuentra principalmente en el nivel conceptual que conceptualizan las innovaciones de blockchain en negocios y en el nivel prescriptivo que describe las aplicaciones comerciales de la cadena. La investigación en el nivel descriptivo está rezagada, ya que se necesitan más esfuerzos para descubrir nuevas explicaciones y teorías subyacentes al fenómeno blockchain. Por ejemplo, hay una necesidad de determinar la validez económica y social de las aplicaciones blockchain. La investigación de Blockchain proviene de varias disciplinas relevantes, tal como científicas, comerciales y aplicaciones tecnológicas. Inicialmente, la investigación en blockchain comienza con técnicas y problemas de negocios, y se involucrarán más disciplinas a medida que los impactos de blockchain penetren profundamente en la sociedad y los gobiernos (Zhao, Fan, & Yan, 2016).

6.2. Blockchain

Blockchain es un ledger distribuido creado por bloques que contienen detalles de transacciones conectados en orden cronológico para formar una serie de cadena. Es un libro mayor distribuido en el cual los participantes de la red peer-to-peer (P2P) de Blockchain, y no el administrador central, genera bloques. Las posibilidades de uso de Blockchain son reconocidas en muchos campos diferentes, lo que resulta en muchos desarrollos y estudios que se llevan a cabo, y las inversiones están sucediendo activamente. Blockchain es una tecnología para asegurar la integridad y confiabilidad de los registros de transacciones sin tercero como proveedor de servicios de confianza, haciendo que todos los participantes de la red creen, graben, almacenen y verifiquen la información de la transacción conjuntamente, y tiene la estructura para realizar diversos servicios de aplicaciones basados en infraestructura de red distribuida, utilizando tecnologías de seguridad incluyendo Hash, firma digital y criptografía. La tecnología Blockchain fue diseñada para guardar y usar una criptomoneda llamada Bitcoin de manera segura. (Zhao, Fan, & Yan, 2016).

Blockchain es un sistema que permite escribir movimientos de tokens en un gran libro virtual que funciona a modo de libro de contabilidad para una moneda. Este libro ha demostrado ser intocable, gracias a estar completamente distribuido y constantemente actualizado con las nuevas entradas contables que se producen. Las entradas contables se agrupan por bloques antes de ser escritas en gran libro de contabilidad que es el blockchain. De esta manera blockchain pasa a ser un gran libro de contabilidad que puede ser escrito por cualquier entidad, pero una vez escrito no puede ser modificado, aunque cualquiera puede leerlo (Lérida & Pérez, 2016).

Una amplia gama de activos escasos pueden ser representados por los tokens de Blockchain, como monedas, valores, propiedades, certificados, entre otros. Los tokens de Blockchain generalmente tienen un suministro fijo o siguen un

programa de suministro transparente, lo que los hace antiinflacionarios. Además, pueden transferirse entre partes sin la participación de una entidad central y pueden negociarse en intercambios de divisas digitales sin fronteras. Hay dos tipos principales de tokens de blockchain: moneda y token.

Una moneda suele ser nativa de una cadena de bloques. Dado que la tecnología blockchain se basa en la criptografía, dicha moneda generalmente se denomina criptomoneda. El ejemplo principal es Bitcoin, que es la moneda nativa de la cadena de bloques de Bitcoin (Nakamoto, 2008). El blockchain de Bitcoin permite a los usuarios almacenar y transferir bitcoins en una red de igual a igual. Otro ejemplo es Ether, que es la moneda nativa de la cadena de bloques de Ethereum. Al igual que la cadena de bloques de Bitcoin, la cadena de bloques Ethereum permite a los usuarios almacenar y transferir Ethers en una red Peer-to-Peer (P2P). Además, el blockchain de Ethereum puede potenciar contratos inteligentes y aplicaciones descentralizadas, que deben usar Ether para pagar los servicios computacionales proporcionados por la plataforma Ethereum (Chen & Yan, 2018).

A diferencia de una moneda, un token no es nativo de una cadena de bloques, sino que se crea sobre un blockchain y se rige por un contrato inteligente. En la plataforma Ethereum, por ejemplo, la mayoría de los tokens se rigen por contratos inteligentes siguiendo el estándar común llamado ERC20, que especifica un conjunto de funciones y eventos que deben implementar todos los contratos inteligentes que cumplan con ERC20. Siguiendo el mismo estándar, los tokens ERC20 se pueden reconocer y comprender fácilmente en el ecosistema de Ethereum. Los tokens ERC20 se han creado para representar una amplia gama de activos digitalizados, lo que les permite desempeñar papeles importantes en el ecosistema de Ethereum. El valor de estos tokens depende del valor de los activos y servicios subyacentes que representan estos tokens. Por ejemplo, TenX (2017) es un servicio de pago habilitado con

blockchain; tiene una billetera que permite a los usuarios almacenar sus criptomonedas y una tarjeta que permite a los usuarios gastarlas. TenX ha emitido el token de pago. Los usuarios de la tarjeta TenX pueden ganar el token de pago, al igual que los usuarios de tarjetas de crédito pueden ganar puntos de recompensa (Chen & Yan, 2018).

6.3. 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 (Viriyasitavat & Hoonsopon, 2018). De esta manera tenemos blockchain públicas, privadas e híbridas.

Blockchain Públicas: son de tipo abierto, en el que cualquiera puede participar. Todos los participantes pueden acceder libremente a datos y realizar transacciones, pero dado que numerosos usuarios no verificados están participando, se necesita cifrado y verificación avanzadas, y por lo tanto, la expansión de la red se torna lenta y difícil. Además, 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 sistema de gestión (Oh & Shong, 2017). También permiten que cualquiera acceda y mantenga el libro mayor distribuido con permisos para validar la integridad ejecutando un mecanismo de consenso. 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 (Viriyasitavat & Hoonsopon, 2018).

Blockchain Privadas: en ella el propietario genera y maneja el Blockchain. Esto es apropiado si el propietario desea administrar la Blockchain como el sistema centralizado (Oh & Shong, 2017). 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 (Viriyasitavat & Hoonsoon, 2018).

Blockchain Híbridas (Consortio): 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 (Oh & Shong, 2017).

La Blockchain híbrida es adecuada para sistemas semicerrados compuestos por unas pocas empresas, a menudo organizadas en forma de consorcio. El grado de apertura de los datos varía, por lo general con controles de acceso, definidos por el consorcio, para controlar el acceso en ambos participantes y la información dentro de Blockchains. A pesar de que el sistema no está completamente abierto, los beneficios de la descentralización se pueden obtener parcialmente. Hyperledger Fabric, Ripple y Stellar son ejemplos de implementaciones de Blockchain Híbridas (Viriyasitavat & Hoonsoon, 2018).

Por lo tanto, las instituciones financieras están prestando atención a Blockchain Híbridas y Privadas que aprovecharán al máximo ventajas de Blockchain, como la reducción de costos, sin perder la autoridad de control del sistema e iniciativa, que son necesarios en el servicio financiero.

Tipos de Blockchain	Blockchain Pública	Blockchain Híbrida	Blockchain Privada
Entidad gestora	Todos los participantes (descentralización)	Participantes que pertenezcan al consorcio.	Una institución central tiene toda la autoridad.
Gobernanza	Es muy difícil cambiar la regla que se ha hecho.	Las reglas podrían cambiarse con relativa facilidad de acuerdo con el acuerdo entre los participantes del consorcio.	Las reglas podrían cambiarse fácilmente de acuerdo con la decisión tomada por la institución central.
Velocidad de transacción	Es difícil expandir la red y la velocidad de transacción es lenta.	Es fácil expandir la red y la velocidad de transacción es rápida.	Es muy fácil ampliar la red y la velocidad de transacción es rápida.
Acceso a los datos	Cualquiera puede acceder	Solo usuarios autorizados pueden acceder	Solo usuarios autorizados pueden acceder
Identificabilidad	Seudo-anónimo	Identificable	Identificable
Prueba de transacción	La entidad para la prueba de la transacción se decide mediante algoritmos como PoW y PoS, y no se puede conocer de antemano.	La entidad para la prueba de la transacción se conoce a través de la autenticación, y la verificación de la transacción y generación de bloques se realizan de acuerdo con las reglas acordadas de antemano.	La prueba de transacción es realizada por la institución central.
Casos de utilización	Bitcoin	R3CEV	Linq, una plataforma de mercado bursátil para compañías sin cotización NASDAQ

Cuadro N°1. Características según tipo de blockchain. Fuente: Oh & Shong (2017).

A diferencia de Blockchain Públicas, que proporciona pseudoanonimato, es posible identificar el sujeto en Blockchain Privadas. Las transacciones se manejan rápidamente, la expansión de la red es fácil y podría ser modificada de la manera que el usuario desee, y por lo tanto, es adecuado para servicios financieros. Por lo tanto, está recibiendo atención de las compañías e instituciones (Oh & Shong, 2017). El Cuadro N°1, presenta las características de cada tipo de blockchain.

Según (Viriyasitavat & Hoonsopon, 2018), todos los tipos de Blockchain comparten las siguientes similitudes con respecto a los beneficios que ofrece esta tecnología:

- Operan en una red P2P que proporciona cierto grado de descentralización,
- Múltiples nodos mantienen la integridad del libro mayor a través de mecanismos de consenso,
- Los datos se almacenan en Blockchain que proporciona inmutabilidad, incluso cuando algunos nodos son defectuosos o maliciosos.

6.4. ¿Por qué es tan innovador?

La tecnología blockchain como base para libro mayor distribuidos ofrece una innovadora plataforma para un nuevo mecanismo de transacciones descentralizado y transparente en industrias y negocios. Las características heredadas de esta tecnología mejoran la confianza a través de la transparencia y la trazabilidad dentro de cualquier transacción de datos, bienes y recursos financieros. A pesar de las dudas iniciales sobre esta tecnología, Recientemente, los gobiernos y las grandes corporaciones han investigado para adoptar y mejorar esta tecnología en varios dominios de aplicaciones, desde las finanzas, las industrias sociales y legales, hasta el diseño, fabricación y redes de la cadena de suministro (Abeyratne & Monfared, 2016).

A grandes rasgos, lo realmente innovador de blockchain es que su sistema permite escribir los movimientos de tokens (por ejemplo bitcoins) en un gran libro virtual que funciona a modo de gran fichero de contabilidad para una moneda. Ese libro ha demostrado ser inatacable, y se basa en estar completamente distribuido y ser actualizado constantemente con las nuevas entradas contables que se van produciendo. Esas entradas contables se

agrupan por bloques antes de escribirse en el gran libro de contabilidad que es el blockchain. Es decir, blockchain es una especie de gran libro de contabilidad que puede ser escrito por cualquier entidad, pero que una vez escrito no hay forma de modificarlo, aunque cualquiera puede leerlo.

La unión de los bloques en los que se agrupan los apuntes de contabilidad es lo que se conoce como cadena de bloques o blockchain. Es decir, el blockchain es un gran libro de contabilidad que se va incrementando conforme se van produciendo movimientos y que se caracteriza porque una vez que se crea un movimiento de tokens y se inscriben, este movimiento nunca podrá ser modificado por nadie, lo que le da legitimidad y la posibilidad de gestionar transacciones entre personas que no se conocen a través de redes que son inseguras originalmente.

La primera criptomoneda exitosa Bitcoin se basó en la tecnología blockchain. Y desde entonces se sabe que el blockchain es una base de datos distribuida para todas las transacciones y resuelve el problema del doble gasto combinando la tecnología peer-to-peer con criptografía de clave pública. Literalmente, un blockchain es una cadena de bloques de información que registra las transacciones de Bitcoin. Los algoritmos de creación y la infraestructura computacional, para insertar y usar los bloques se consideran como la tecnología blockchain. La característica clave principal de la tecnología blockchain es la capacidad de rastrear transacciones dentro de bases de datos públicas descentralizadas y, por lo tanto, excluye la falsificación y el fraude. La esencia de blockchain radica en su capacidad para admitir transacciones confiables a través de redes computacionales en lugar de supervisión y control humano. El consenso distribuido y el anonimato son dos importantes características de la tecnología blockchain. Una serie de grandes compañías industriales, como IBM, Microsoft, Intel y NEC invierten actualmente en la

explotación de blockchain para enriquecer su cartera de productos (Efanov & Roschin, 2018).

6.4.1. Ventajas y Desventajas

Blockchain proporciona intrínsecamente varias ventajas tecnológicas clave para los usuarios que son implicaciones de su arquitectura estructural. Algunos de los cuales incluyen durabilidad, transparencia, inmutabilidad e integridad del proceso (Abeyratne & Monfared, 2016):

- **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.

Sin embargo, esta tecnología requiere cierta infraestructura de TI para todos los actores, como el acceso a Internet, que puede ser poco práctico en este momento para algunos proveedores remotos de materia prima. Los perfiles digitales tendrían que mantenerse actualizados constantemente a través de sistemas manuales o automatizados, como etiquetas simples o RFID. Los contratos inteligentes deben implementarse y ser incrustado en el sistema para proporcionar incentivos que permitan a blockchain controlar el progreso de un proceso de negocios. En adición, la capacidad de desempeño de dicho sistema puede ser un cuello de botella para la implementación de la solución propuesta (Abeyratne & Monfared, 2016).

Características de Blockchain	Ventajas	Desventajas
P2P	Las transacciones P2P son posibles sin la confianza de un tercero como proveedor de servicio. Reducción de tarifas innecesarias.	Cuando ocurre un problema, no se sabe quién es el responsable de ello.
Escalabilidad	Fácilmente establecido, conectado y expandido por fuente distribuida. El costo de desarrollo del sistema es reducido.	El número posible de transacciones que se pueden manejar con el pago es reducida en comparación con la escala de transacción dentro de la economía real
Transparencia	Es posible acceder públicamente a todos los registros de transacciones. Legalización de transacciones y reducción de los costos de regulación.	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 reidentificación mediante la combinación es posible.
Seguridad	El libro mayor es de propiedad conjunta (integridad) El costo relacionado con la seguridad se reduce.	Cuando se pierde la clave privada o es hackeada, no existe una solución general. No proporciona confidencialidad.
Estabilidad del Sistema	No hay un único punto de falla. Si se producen errores o disminución de la función en ciertos sistemas participantes, el efecto en toda la red es muy leve.	Focalizada en grandes grupos mineros. Es difícil ejecutar en tiempo real manejo de gran volumen.

Cuadro N°2. Ventajas y desventajas según características de Blockchain.

Fuente Oh & Shong (2017).

6.5. Entorno Blockchain

Se pueda pensar que blockchain es una tecnología permitida para gestionar y realizar pagos a través de Internet utilizando moneda virtual, pero eso es sólo el principio del ecosistema y de las posibilidades. Lo que permite básicamente blockchain es la generación de un entorno de confianza entre pares que elimina la necesidad de intermediarios y que es soportado por toda la comunidad. Este entorno de confianza permite el intercambio de activos de cualquier tipo, no sólo moneda virtual. Bitcoin, la primera aplicación desarrollada para blockchain, permite el intercambio de un token o moneda virtual denominada bitcoin, pero hay otras aplicaciones que permiten el intercambio de otros activos como nombres de dominio, propiedades, oro, etc. El intercambio viene definido por un sentido de la propiedad totalmente definido ya que todo queda almacenado en los blockchain particulares que una vez escritos resultan inalterables, pero que permiten de forma permanente la lectura pública de sus datos (Lérida & Pérez, 2016).

Hoy en día se pueden identificar las siguientes tres generaciones del desarrollo de la cadena de bloques: Blockchain 1.0 como moneda digital, Blockchain 2.0 como economía digital y Blockchain 3.0 como sociedad digital (Efanov & Roschin, 2018). Curiosamente, Blockchain 1.0 tomó unos pocos años para madurar a partir de 2008, Blockchain 2.0 y 3.0 han surgido casi en paralelo de manera explosiva en 2015. Sin embargo, mientras muchos proyectos experimentales han proliferado, tomará algunos años para que Blockchain 2.0 y 3.0 se apoderen y puedan crear impactos económicos reales (Zhao, Fan, & Yan, 2016).

6.5.1. Blockchain 1.0

Blockchain 1.0 es moneda, el despliegue de criptomonedas en aplicaciones relacionadas con el efectivo, como los sistemas de transferencia de moneda, remesas y pagos digitales (Swan, 2015). Es la primera generación de aplicaciones de tecnología blockchain, básicamente está pensado para las transacciones económicas y pagos (Lérida & Pérez, 2016). Se refiere a la plataforma de tecnología subyacente (minería, hashing y el libro mayor público), protocolo de superposición (es decir, software de habilitación de transacciones) y la moneda digital (bitcoin u otras) que representan un almacén de valor y proporcionan valor al protocolo por sí mismo. Bitcoin es un caso raro en el que la práctica parece estar por delante de la teoría. Según Efanov & Roschin (2018) las principales ventajas de Bitcoin son:

- Ofrece la posibilidad de tarifas de transacción considerablemente reducidas para compras en línea.
- Bitcoin proporciona mayor anonimato que las tarjetas de crédito. Las cuentas son seudoanónimas y el protocolo está diseñado para fomentar el uso de nuevos números de cuenta para cada transacción.
- El diseño descentralizado de Bitcoin y otras monedas digitales protege contra la inflación. Las monedas tradicionales dependen de un banco central para regular el suministro de dinero, introduciendo dinero nuevo en circulación según sea necesario. Bitcoin, por el contrario, usa la criptografía para garantizar un suministro de dinero relativamente fijo, que se permite crecer a intervalos regulares.

6.5.2. Blockchain 2.0

Supone el paso de las criptomonedas al mundo de las aplicaciones reales. Está pensado para la gestión y transferencia de activos y cualquier otro tipo de bien que pueda estar en un registro público. Igualmente se puede utilizar para gestión y transferencia de activos físicos siempre que los mismos puedan ser codificados de alguna manera (Lérida & Pérez, 2016).

Aunque el concepto de economía digital se propuso hace más de 20 años, solo hoy cuenta con una plataforma tecnológica apropiada. Blockchain 2.0 se refiere a la amplia gama de aplicaciones económicas y financieras existentes más allá de simples pagos, transferencias, y transacciones. Dichas aplicaciones incluyen instrumentos bancarios tradicionales, como préstamos e hipotecas, complejos instrumentos del mercado financiero como acciones, bonos, futuros, derivados, además instrumentos legales tal como títulos, contratos y otros bienes y propiedades que pueden ser monetizado. El sistema de compensación de pagos y los sistemas de información de crédito bancario pueden ser escenarios apropiados de la aplicación blockchain. Un caso de uso emergente clave de la tecnología blockchain involucra contratos inteligentes. Estos contratos Inteligente son básicamente programas de computadora que pueden ejecutar automáticamente los términos de un contrato. Cuando se cumple una condición preestablecida en un contrato inteligente entre entidades participantes, las partes involucradas en el acuerdo contractual pueden realizar pagos automáticamente según el contrato de manera transparente (Efanov & Roschin, 2018).

Parte de la terminología que se refiere ampliamente al espacio Blockchain 2.0 puede incluir Bitcoin 2.0, protocolos Bitcoin 2.0, contratos inteligentes, propiedad inteligente, Dapps (aplicaciones descentralizadas), DAO

(organizaciones autónomas descentralizadas) y DAC (corporaciones autónomas descentralizadas) (Swan, 2015).

6.5.3. Blockchain 3.0

Son aplicaciones de blockchain que van más allá de la moneda, las finanzas y los mercados, especialmente en las áreas de gobierno, salud, ciencia, alfabetización, cultura y arte (Swan, 2015). Corresponde al desarrollo de nuevas tecnologías basadas en la identidad, la libertad, la democracia y la contabilidad de activos de cualquier tipo. Blockchain 3.0 tratará de solucionar las restricciones que actualmente existen en los mercados a nivel local, regulatorio y de entornos macroeconómicos. Es decir, mientras que blockchain 2.0 está tratando de migrar aplicaciones del mundo digital utilizando la trazabilidad y posibilidades de contabilidad en mercados masivos, blockchain 3.0 tratará de cambiar el statu quo establecido utilizando la potencia, la deslocalización y la ubicuidad que generan las tecnologías blockchain. Si se puede hablar de blockchain 2.0 como una evolución, en el caso de blockchain 3.0 se debe hablar de revolución. (Lérida & Pérez, 2016). Blockchain 3.0 se refiere a una gran variedad de aplicaciones que no involucran dinero, divisas, mercados financieros u otra actividad económica. Tales aplicaciones incluyen arte, salud, ciencia, identidad, gobernanza, educación, bienes públicos y diversos aspectos de la cultura y la comunicación. La aplicación más prometedora de la tecnología blockchain está relacionada con las smart cities, que involucra elementos horizontalmente acumulativos, como la gobernanza inteligente, la movilidad inteligente, la vida inteligente, el uso inteligente de recursos naturales, ciudadanos inteligentes y economía inteligente (Efanov & Roschin, 2018).

6.6. La seguridad de Blockchain

6.6.1. El problema del 51%

Todo el mecanismo que tiene una DApp para su funcionamiento tiene un punto débil que se conoce de antemano y de difícil resolución: el problema del 51%. Cuando más del 51% de la tasa de hash está controlada por un solo nodo (un minero o grupo de mineros), la cadena de bloques se puede distorsionar maliciosamente. El ataque del 51% también resulta en una bifurcación, que es donde hay dos bloques conflictivos compitiendo para la adición a la cadena de bloques (Lérida & Pérez, 2016). Si se modifica un bloque en medio del Blockchain, los enlaces hash no coincidirán y deberán crear nuevamente. Para hacer esto, los bloques posteriores deben ser re-minados para incluir los nuevos hashes que se deben volver a calcular. En el caso entonces que un atacante quisiera modificar un valor por su beneficio e intente reconstruir la cadena modificada calculando los hashes, debería tener el control de al menos el 51% del recurso que utilice el protocolo de consenso, para que pueda reconstruir la cadena a una velocidad superior a la que ésta se genera. Esta vulnerabilidad afecta principalmente a las plataformas que utilizan prueba de trabajo o prueba de participación, pero aun así es una situación difícilmente realizable, dado que significaría tener el 51% de la potencia computacional o el 51% de las cryptomonedas de toda la red (Sanz, 2017).

6.6.2. Doble Gasto

La tecnología Blockchain resuelve un importante problema informático que había sido una barrera para tener un sistema monetario digital funcional durante años: el problema del doble gasto (Nakamoto, 2008). El problema del doble gasto es que el dinero solo debe gastarse una vez, a diferencia de un archivo, que puede ser copiado arbitrariamente muchas veces (Melanie Swan, 2018).

El doble gasto ocurre cuando alguien hace más de un pago usando un cuerpo de fondos. Esto es posible en una red peer-to-peer porque puede haber retrasos de propagación cuando los pagos pendientes se transmiten a la red o a las redes y los nodos reciben transacciones no confirmadas en diferentes momentos. Blockchain aborda este problema requiriendo que los nodos mineros resuelvan un problema matemático complejo para verificar la transacción. La complejidad del cálculo se ajusta de modo que, en promedio, se necesita 10 minutos para resolver un problema utilizando los poderes de procesamiento de los mineros. Porque solo bloques con respuestas correctas al problema matemático se pueden agregar a la cadena, solo uno entre los pagos múltiples es aceptado y registrado en la blockchain, por lo que es casi imposible para las partes gastar fondos doblemente. Los sistemas centralizados de almacenamiento y administración de datos son susceptibles de piratería, intrusión e incumplimientos, pero el mecanismo de consenso distribuido blockchain evita el hackeo. Cada transacción debe ser verificada por la comunidad de mineros, dejando transacciones fraudulentas que no pueden pasar la verificación colectiva y validación porque blockchain es constantemente monitoreada por toda la red de nodos, cada uno de los cuales mantiene una copia de la cadena de bloques, los usuarios maliciosos no tienen forma de insertar bloques fraudulentos en el libro de contabilidad público sin ser notado inmediatamente por otros. Por lo tanto, es imposible comprometer la integridad de los registros en el blockchain (Efanov & Roschin, 2018).

6.6.3. Claves Privadas

Un aspecto clave en la seguridad es la gestión y almacenaje de claves privadas. Sin estas claves privadas no es posible realizar transacciones con las direcciones, con lo que la pérdida de estas es sinónimo de perder los fondos. Si las claves se pierden o destruyen no hay forma de recuperarlas y los fondos asociados a esas direcciones nunca se podrán utilizar. Si las claves son

obtenidas por un tercero podrá hacer uso fraudulento de todos los fondos asociados (Gimeno, 2018). En consecuencia, todos los activos que esta persona posee en el blockchain desaparecerán, y será casi imposible identificar al ladrón. Las consecuencias pueden ser más devastadora que el robo de identidad en el mundo fuera de línea, donde las instituciones de terceros (por ejemplo, compañías de tarjetas de crédito) o las autoridades centrales resguardan transacciones, controlan riesgos, detectan actividades, o ayudan a encontrar culpables (Efanov & Roschin, 2018).

7. Aplicaciones Blockchain

Desde el descubrimiento de la tecnología blockchain, este campo ha experimentado un crecimiento masivo a través de varios conceptos innovadores y tecnológicos. Inicialmente, esta tecnología ganó una reputación negativa debido a su asociación con compras imposibles de rastrear en la 'red oscura' donde los usuarios usarían monedas digitales como Bitcoin para realizar compras de forma anónima. Sin embargo, en los últimos años, muchas grandes empresas como IBM, JPMorgan y Barclays han invertido en investigación y desarrollo de la tecnología Blockchain. Debido a tal interés de las principales organizaciones, y la gran cantidad de dinero circulando en criptomonedas, empresarios, organizaciones innovadoras y creativas han sido atraídos por este nuevo campo de la tecnología de la información. Este rápido crecimiento en el campo ha cambiado la perspectiva de muchos gobiernos para ver el potencial de esta tecnología por sobre su relación inicial con actividades ilegales (Abeyratne & Monfared, 2016). El interés corporativo, industrial y gubernamental en las tecnologías Blockchain ha crecido considerablemente porque las aplicaciones se extienden mucho más allá del dominio de las criptomonedas.

Según Swan (2018) existen cuatro clases principales de aplicación para la tecnología Blockchain:

1. Activos monetarios (moneda, pagos, remesas, finanzas, valores e instrumentos financieros),
2. Propiedad (terrenos, bienes raíces y registros de títulos de auto),
3. Contratos (acuerdos comerciales, licencias, registro, testamentos y fideicomisos, acuerdos de asociación y registro de propiedad intelectual)
4. Credenciales de identidad (pasaporte, visa, licencia de conducir y registros de nacimiento).

7.1. Escenarios integrados de IoT y Blockchain

La tecnología de Internet de las Cosas (IoT) en conjunto con Blockchain pueden proporcionar increíbles oportunidades para el desarrollo de aplicaciones descentralizadas para la economía compartida (Huckle, Bhattacharya, White, & Beloff, 2016). IoT ha generado nuevas oportunidades a la comunidad, como mecanismos para acceder y compartir información. En este sentido Blockchain puede enriquecer la IoT, proporcionando un servicio de intercambio confiable, donde la información es confiable y puede ser trazable. Las fuentes de datos pueden ser identificadas en cualquier momento y los datos permanecen inmutables en el tiempo, aumentando su seguridad. La unión de ambas tecnologías puede brindar descentralización y escalabilidad, identidad, autonomía, confiabilidad, seguridad y una diversidad de usos como se puede apreciar en el Cuadro N°3 (Reyna, Martín, Chen, Soler, & Díaz, 2018).

Aplicación	Clasificación	Plataforma
LO3 Energy	Energía Microgrid	Ethereum
ADEPT	Contratos inteligentes con dispositivos IoT	Ethereum
Slock.it	Alquilar / vender / compartir objetos inteligentes	Ethereum
Aigang	Red de seguros para activos IoT	Ethereum
MyBit	Inversión en dispositivos IoT	Ethereum
AeroToken	Compartiendo el mercado del espacio aéreo para navegación con drone	Ethereum
Chain of things	Identidad, seguridad e interoperabilidad	Ethereum
Chronicled	Identidad, procedencia de datos y automatización	Multiplataforma
Modum	Integridad de datos para la cadena de suministro	Multiplataforma
Riddle and Code	Economía compartida e IoT	Multiplataforma
Blockchain of things	Conectividad segura entre dispositivos IoT	Multiplataforma

Cuadro N°3. Aplicaciones IoT y Blockchain. Fuente: Reyna & Martín (2018).

7.2. Blockchain e Instituciones Financieras

Las tareas existentes de las instituciones financieras se decidieron por el libro mayor administrado por una institución específica, independientemente de si hubo un almacenamiento real de la propiedad de los activos. En el depósito a la vista, que representa la mayor parte de la moneda que circula hoy, los bancos administran el saldo para cada cliente, aprobando y registrando depósitos y retiros, y el banco central registra en el libro de contabilidad el saldo de cada banco y maneja las transferencias de fondos entre ellos. Por lo tanto, tiene que asumir el costo de gestión para evitar que la confianza en el sistema se dañe debido a problemas tales como manipulación y hackeo de información. Blockchain no requiere un tercero en el medio, por lo tanto puede generar la reducción de las tarifas y el costo de gestión, y la información es de propiedad conjunta, por lo que es difícil manipular arbitrariamente (Oh & Shong, 2017). En este sentido debido a la dura competencia en la actual economía el sector de servicios financieros debe innovar para reducir los costos de transacción y por consiguiente está liderando el camino para la utilización de Blockchain. Esta tecnología ha sido propuesta como una solución innovadora a áreas como compensación y liquidación de activos financieros, sistemas de pago, contratos y riesgos operacionales en el mercado financiero (Zhao, Fan, & Yan, 2016). Sin

embargo, las instituciones financieras están introduciendo Blockchain para mejorar el manejo de los procesos de información en lugar de construir un sistema Blockchain descentralizado a gran escala para innovar el modelo de negocio actual (Oh & Shong, 2017). Algunas aplicaciones actuales son:

- **Monedas:** Las monedas digitales como Bitcoin fueron el primer caso de uso de la tecnología blockchain, ofreciendo un sistema completamente descentralizado, emisión de moneda y pagos detectables. Tras el creciente éxito de Bitcoin, un gran número de monedas digitales se han creado, que son variaciones de la arquitectura del sistema Bitcoin. Actualmente hay más de 600 monedas digitales diferentes que utilice la tecnología blockchain como su capa de tecnología subyacente. Las monedas digitales siguen siendo el caso de uso más popular de La tecnología blockchain, sin embargo, los avances e innovaciones en este campo, han llevado a muchos otros casos de uso (Abeyratne & Monfared, 2016).
- **Intercambios:** Blockchain se puede usar para crear sistemas descentralizados, que facilitan el intercambio o las monedas digitales como Bitcoin, o el intercambio de cualquier otra forma de activo que pueda registrarse con su propia identidad digital en una red. Compañías tales como Coinbase, ItBit o Kraken son ejemplos de intercambios de divisas digitales que existen actualmente (Abeyratne & Monfared, 2016).
- **Mercado de valores:** los mercados bursátiles descentralizados pueden ser impulsados a través de la tecnología blockchain, donde las acciones pueden negociarse en una plataforma que no está controlada por un único organismo de gobierno en oposición a los sistemas actuales. Los usuarios pueden estar seguros de que los intercambios se llevan a cabo correctamente ya que el sistema solo funcionará como se describe en el protocolo. Sin embargo, esta aplicación aún no ha sido adoptada (Abeyratne

& Monfared, 2016). Una aplicación blockchain exitosa en el mercado financiero es chain.com, que es una startup respaldada por NASDAQ. Su objetivo es proporcionar un plataforma para el intercambio de capital privado sobre blockchain (Zhao, Fan, & Yan, 2016).

- **Remesas:** El servicio internacional de remesas, en el cual los clientes tienen que pagar una alta tarifa, es reconocido como el campo donde la tecnología Blockchain es más útil, donde las transacciones entre las personas sin intermediario son posibles. (Oh & Shong, 2017).

7.3. Contratos inteligentes

Un contrato inteligente es un programa informático que ejecuta acuerdos establecidos entre dos o más partes haciendo que ciertas acciones sucedan como resultado de que se cumplan una serie de condiciones específicas. Es decir, cuando se da una condición programada con anterioridad, el contrato inteligente ejecuta automáticamente la cláusula correspondiente (miethereum, 2018). En el contexto de blockchain, los contratos o contratos inteligentes significan transacciones de blockchain que van más allá de simples transacciones de compra / venta de divisas, y pueden tener instrucciones más extensas incorporadas en ellos. En una definición más formal, un contrato es un método de uso de Bitcoin para establecer acuerdos con personas a través de la cadena de bloques. Un contrato en el sentido tradicional es un acuerdo entre dos o más partes para hacer o no hacer algo a cambio de otra cosa, los contratos inteligentes poseen tres elementos que los diferencian con respecto a un contrato tradicional la autonomía, la autosuficiencia y la descentralización. (Swan, 2015).

7.4. Aplicaciones Sociales

- **Identidad digital:** la tecnología Blockchain podría proporcionar la infraestructura para escalar la identidad digital a un costo extremadamente bajo, con mejoras significativas en la seguridad. En lugar de que varios gobiernos expidan identidades o pasaportes a los ciudadanos. El servicio de identidad descentralizado sobre el uso de la tecnología blockchain puede brindar a los usuarios de todo el mundo la posibilidad de obtener su propia identidad digital a través de un sistema descentralizado. Esta aplicación había llamado la atención de muchas organizaciones gubernamentales (Abeyratne & Monfared, 2016).
- **Votación:** la tecnología blockchain mediante el uso de "claves privadas" para cada votante puede usarse para autenticar la votación proceso. En esta aplicación, el protocolo del sistema se puede diseñar de modo que las identidades de los usuarios se puedan validar pero se mantengan anónimo mientras se calcula el resultado final de las elecciones en tiempo real. Dado que el protocolo es transparente, los votantes pueden estar seguros que los resultados son precisos y no son vulnerables a la manipulación y el fraude (Abeyratne & Monfared, 2016). En 2015, Fundación Bitcoin comenzó un nuevo proyecto que tiene como objetivo desarrollar una votación basada en blockchain, que "proporciona una mayor transparencia en el proceso de votación, con cada votación registrada en el blockchain " (Zhao, Fan, & Yan, 2016).

7.5. Aplicaciones Legales

El entorno legal de blockchain parecen estar entre los temas más controvertidos en torno a esta novedosa tecnología, que crean incertidumbres en cuanto al alcance y la velocidad de su eventual adopción (Gönenç Gürkaynak, 2018). Los

avances tecnológicos ofrecidos por blockchain prometen amplias gamas de uso en una variedad de sectores y áreas legales, incluida:

- **Contratos inteligentes:** la idea es relativamente sencilla: un protocolo de software realiza una acción (libera fondos, envía información, hace compra, etc.) cuando se cumplen ciertas condiciones (se recibe un pago, se determina el resultado de un evento, etc.). La ventaja de los contratos basados en blockchain es que reducen la cantidad de participación humana requerida para crear, ejecutar y hacer cumplir un contrato, lo que reduce su costo al tiempo que aumenta la seguridad de los procesos de ejecución y cumplimiento (Abeyratne & Monfared, 2016).
- **Propiedad intelectual:** Las identidades digitales se pueden crear para cualquier activo físico del mundo que esté representado en el sistema blockchain. Usando estas identidades, la propiedad se puede controlar a través de contratos inteligentes, por ejemplo, la puerta de la habitación en un hotel puede estar desbloqueada automáticamente cuando se acepta el pago del usuario (Abeyratne & Monfared, 2016), o un automóvil que no permite al usuario conducir, si su seguro está vencido (Huckle, Bhattacharya, White, & Beloff, 2016).

7.6. Cadena de Suministro

En la gestión de la cadena de suministro, la tecnología blockchain proporciona una solución innovadora a la procedencia del producto (Zhao, Fan, & Yan, 2016). La llegada de blockchain se establece para transformar las actividades de la cadena de suministro, es probable que blockchain afecte los objetivos clave de la gestión de la cadena de suministro, como el costo, calidad, velocidad, confiabilidad, reducción del riesgo, la sostenibilidad y la flexibilidad

(Kshetri, 2018). Hay miles de millones de productos que se fabrican todos los días a nivel mundial, a través de cadenas de suministro complejas que se extienden a todas las partes del mundo. Sin embargo, hay muy poco conocimiento de cómo, cuándo y dónde se originaron, fabricaron y utilizaron estos productos a través de su ciclo de vida. Incluso antes de llegar al consumidor final, los bienes viajan a través de una vasta red de minoristas, distribuidores, transportadores, instalaciones de almacenamiento y proveedores que participan en el diseño, la producción, la entrega y las ventas. Sin embargo estos viajes siguen siendo una dimensión invisible de nuestras posesiones. Las cadenas de suministro son cada vez más complejas, extendidas y globales. Un evento en un extremo del mundo puede detener la producción o entrega de un servicio en el otro extremo. Las consecuencias por fallas en la cadena de suministro pueden ser muy perjudiciales para las empresas, tanto desde el punto de vista financiero como en términos de reputación. La tecnología blockchain puede mejorar potencialmente la transparencia y los problemas de trazabilidad dentro de la cadena de suministro de fabricación mediante el uso de registros inmutables de datos, almacenamiento distribuido y accesos de usuarios controlados. (Abeyratne & Monfared, 2016).

Las actividades de la cadena de suministro se encuentran entre las que tienen más probabilidades de ser transformadas por blockchain, facilitando la medición válida y efectiva de los resultados y el rendimiento de los procesos clave de la cadena de suministro. La industria alimentaria es la que posee mayor probabilidad de ser transformada. El ejemplo del brote de E.coli 2015 en Chipotle Mexican Grill es ilustrativo de un problema generalizado que enfrenta la cadena de suministro de alimentos. En este sentido, un elemento clave del modelo basado en blockchain es que todas las transacciones son auditables, lo que es particularmente importante para ganar la confianza de todas las partes interesadas (Kshetri, 2018).

7.7. Sustentabilidad

Estándares y certificaciones son importantes para brindar al consumidor una mejor comprensión del ciclo de vida del producto. Sin embargo, el resultado final es un simple logotipo de la certificación impreso en los productos, aceptado por los consumidores sin poder verificar o comprender el verdadero significado. Auditorías de certificación fallidos por procesos costosos, sumado a regiones con alto nivel de corrupción, deterioran la credibilidad de los procesos y estándares. Algunos ejemplos que atentan contra la sustentabilidad son: los escándalos de emisiones como Volkswagen 2015 y Nissan 2016, daño ambiental, trabajo no ético, trabajo infantil, productos falsificados (Abeyratne & Monfared, 2016). Es particularmente importante para los consumidores percibir la información en los productos del proceso de suministro de materias primas para la entrega del producto a los clientes. (Supranee & Rotchanakitumnuai, 2017). La visibilidad de la cadena de suministro es un desafío empresarial clave, ya que la mayoría de las empresas tienen poca o ninguna información sobre sus proveedores. La transparencia y la visibilidad de la cadena de suministro de extremo a extremo pueden ayudar a modelar el flujo de productos a partir de materias primas, fabricación y productos terminados, lo que permite nuevos tipos de análisis de operaciones, riesgos y sostenibilidad (Abeyratne & Monfared, 2016).

Blockchain cuenta con el potencial para hacer frente al problema antes señalado. Sin embargo, blockchain tiene una serie de desafíos importantes que superar. Primero, la cadena de suministro global opera en un entorno complejo que requiere que varias partes cumplan con diversas leyes, regulaciones e instituciones. Incluyen leyes y regulaciones marítimas, códigos comerciales, leyes relativas a la propiedad y posesión de múltiples jurisdicciones en las rutas de envío. Dado que los negocios internacionales operan en el contexto de estas antiguas leyes, costumbres e instituciones establecidas que son administradas

por seres humanos, la implementación de soluciones basadas en blockchain puede ser una tarea extremadamente compleja (Kshetri, 2018).

7.8. Otras Aplicaciones

Seguimiento de activos: Blockchains se pueden utilizar para rastrear activos físicos, lo que permite mantener un registro de propiedad para cada uno. Everledger es una compañía que rastrea los diamantes mediante la creación de una identidad digital combinando la tecnología blockchain con un profundo conocimiento del dominio a través de asociaciones estratégicas de la industria, entregando identidad a los activos físicos, permitiendo que los artículos tengan pruebas de autenticidad, existencia y propiedad. Proporcionando confianza en la información capturada y rastreada durante su viaje (Abeyratne & Monfared, 2016).

Industria Automotriz: Los fabricantes de piezas de automóviles han invertido en investigación y desarrollo para la innovación de la organización. Debido a las crecientes innovaciones actuales y las presiones sobre los costos de producción, deben determinar cómo evitar gastos innecesarios. Además de ayudar a generar confianza, la aplicación de la tecnología blockchain en el proceso de la cadena de suministro puede ayudar a reducir los costos de las transacciones corporativas y también a prevenir fraudes. Sin embargo, en el diseño del sistema mediante la tecnología para el proceso de la cadena de suministro tanto la integración entre organizaciones, fabricantes de piezas de automóviles y fabricantes de automóviles debe satisfacer las necesidades de diferentes partes interesadas y la naturaleza de los sistemas operativos involucrados en consideración con el fin de aumentar la eficacia de la cadena de suministro (Supranee & Rotchanakitumnuai, 2017).

8. Consideraciones Legales

Características como código abierto, redes públicas y potencial anonimato es lo que hace que los sistemas públicos de blockchain como Bitcoin sean problemáticos desde una perspectiva legal y normativa. Reglas como el conocimiento del cliente para la evaluación de riesgos de ilegalidad y el anti lavado de dinero se ven amenazadas con el pseudoanonimato de blockchain públicas. Así, no es posible que un regulador de servicios financieros pueda verificar el cumplimiento de las reglas antes mencionadas sin involucrar a una entidad central que pueda ser regulada y auditada. La solución a las inquietudes planteadas puede ser el uso de blockchain configurada como consorcio regido por reglas que establecen la base sobre la cual cada parte procesará los datos personales que se incluyen en la cadena de bloques.

Sin lugar a dudas, existe mucho trabajo por hacer con respecto a los datos personales, también con respecto a otras implicaciones legales de blockchain, incluida la función del derecho contractual, por medio de contratos inteligentes, en la gestión de activos y relaciones "dentro de la cadena" y "fuera de la cadena". Hoy es terreno fértil para la colaboración, situación que lo hace atractivo para trabajar en el campo de la legislación y la regulación de la tecnología (Millard, 2018).

9. Marco Teórico del Estado del Arte

La tecnología detrás de blockchain no es nueva, lo realmente innovador desde la perspectiva tecnológica es la forma en que se combinan distintas tecnologías existentes, como las redes peer-to-peer o la encriptación de clave pública (Lérida & Pérez, 2016). El objetivo del protocolo blockchain es conseguir un sistema descentralizado, es decir, compuesto por varios nodos independientes siguiendo el esquema peer to peer (P2P), que gestione un registro único donde se anoten todas las transacciones y operaciones realizadas (Bermúdez, 2016).

9.1. Conceptos Claves

Para entender el funcionamiento de Blockchain primero se deben entender los algunos conceptos claves que se explican en los siguientes apartados.

9.1.1. Red Peer-to-Peer

Una red blockchain está formada por nodos que se comunican con un esquema descentralizado, en el que no existe un elemento orquestador. Se trata de una red de pares, o red entre iguales, donde todos los nodos que forman la red se comportan como iguales entre sí, actuando a la vez como servidores y clientes del resto de nodos de la red. La principal ventaja de las redes peer-to-peer es que son mas solidas frente a posibles contingencias, ya que los nodos funcionan de manera totalmente independientes.

9.1.2. Encriptación de Clave Pública

Este tipo de encriptación tiene doble propósito, el primero es que las direcciones utilizadas para la realización de las transacciones, correspondientes a las direcciones de emisor y receptor de una transacción, son en realidad una

simplificación de la clave pública, de tal forma, que la clave pública realiza la función que la dirección IP tienen en la comunicación en Internet. Cualquier elemento que necesite realizar una transacción en una red blockchain necesita un par clave pública/clave privada para poder enviar y/o recibir transacciones. El otro propósito de emplear la encriptación de clave pública es que todas las transacciones van firmadas digitalmente por el emisor, para garantizar la autoría de la transacción.

9.1.3. Algoritmo de Consenso

Para actualizar el libro mayor, la red debe llegar a un consenso mediante un algoritmo. Llegar a un consenso en una red distribuida significa que todos están de acuerdo con el estado actual del libro mayor (por ejemplo, cuánto dinero tiene cada cuenta) y confirma que nadie está gastando el dinero en forma doble. Llegar al consenso es un problema informático en sistemas distribuidos tolerantes a fallos. Generar un consenso significa que varios servidores en la red distribuida están de acuerdo con el estado de verdad actual del sistema, o en el caso básico de Blockchain, los valores en el libro mayor distribuido. Una vez que las computadoras de la red llegan a una decisión sobre un valor, esa decisión es definitiva. En el contexto informático clásico, los algoritmos de consenso se utilizan para acordar los comandos en los registros de los servidores distribuidos.

El principal problema de las redes descentralizadas es mantener la integridad de la información durante el proceso de actualización de la información que gestionan. Una de las soluciones más populares es la utilización de un algoritmo de consenso que todos los nodos de la red siguen para decidir que nodo es el elegido para actualizar la información. En las redes blockchain se utiliza la prueba de trabajo POW (Proof of Work), que obliga al nodo a realizar un esfuerzo computacional para crear el bloque (Bermúdez, 2016). El primer

nodo que cumpla con la prueba de trabajo lo anuncia en la red con el fin de que el resto de los nodos conozcan quien es el ganador y por lo tanto el nodo que podrá modificar la información.

En las redes Blockchain, los tres tipos principales de algoritmos de consenso para llegar a un consenso de manera distribuida son Prueba de trabajo (POW), Prueba de participación (POS) y Práctica de la tolerancia a falta bizantina (PBFT). La principal innovación del protocolo Blockchain es la estructura de datos sobre un algoritmo de consenso, que permite construir una red distribuida abierta en la que todas las partes pueden llegar a un acuerdo (Melanie Swan, 2018).

- **Prueba de Trabajo POW (Proof of Work):** es un método que sirve para evitar comportamientos malintencionados en un sistema. Para ello, los mineros deben realizar un trabajo que sea muy costoso para ellos, pero fácil de verificar para el resto de la comunidad. Este trabajo es de tipo computacional -informático- y llevarlo a cabo les cuesta poder de procesamiento, que se puede traducir en tiempo, electricidad y hardware (miethereum, 2014). Los algoritmos que operan el sistema distribuido recompensan a los mineros que resuelven problemas matemáticos. El incentivo financiero para cada minero es ser el primero en crear el nuevo bloque de transacciones que las otras máquinas tomarán como el nuevo estado de verdad de la red. El lucrativo registro de transacciones a generado operaciones dedicadas exclusivamente a la minería (Melanie Swan, 2018).
- **Prueba de Transacción POS (Proof of Stake):** el algoritmo de consenso se basa en poseer una participación en la red. En los sistemas POS, el creador de un nuevo bloque se elige de manera determinista, dependiendo de su participación o grado de compromiso (riqueza) en la red. Sin embargo, los sistemas POS son quizás innecesariamente complicados con los niveles

de votación y no necesariamente más eficientes que Bitcoin en términos de lo que podría considerarse un cálculo inútil. Por lo tanto, algunos de los Blockchains de próxima generación están considerando otros métodos.

- **Práctica de la tolerancia a falta bizantina PBFT (Practical Byzantine fault tolerance):** Básicamente, mediante el envío de mensajes entre los nodos ‘validadores’ se intenta averiguar si existe alguno que falla o perturba a la red para aislarlo del sistema. Es la capacidad de un sistema informático distribuido para operar independientemente de los nodos defectuosos (malintencionados o no). PBFT confía en que haya una diversidad de participantes en el sistema distribuido (unos pocos cientos). Para cada bloque en el caso de las transacciones, los algoritmos seleccionan al azar un grupo pequeño y único de usuarios de manera segura y justa. Para protegerlos de los atacantes, las identidades de estos usuarios generalmente se ocultan hasta que se confirma el bloqueo. El tamaño de este grupo generalmente permanece constante a medida que la red crece. (Melanie Swan, 2018). Sin embargo, con este método se pierde en descentralización ya que los nodos validadores que están a cargo de la votación son elegidos por una autoridad central.

9.1.4. Los Mineros

No todos los nodos de una red blockchain participan en resolver el reto de la prueba de trabajo, aquellos nodos que sí participan se conocen como “mineros” ya que el trabajo que realizan estos nodos se asemeja al trabajo de un minero, que debe trabajar para encontrar un metal precioso. Los mineros son computadores que aportan poder computacional a la red, además estos son los encargados de crear los nuevos bloques, a los que incorporan las transacciones que validan, y a su vez tratan de añadirlos a la blockchain. En las redes blockchain, cada vez que un minero consigue resolver el reto recibe una

recompensa por su esfuerzo, ya que al ser redes descentralizadas es la propia red la que debe pagar de alguna forma a los nodos para que estos trabajen para la red (Lérida & Pérez, 2016). Reciben dos tipos de incentivos: las nuevas monedas creadas en el bloque y todas las comisiones de las transacciones incluidas en el bloque (Caballero, 2018).

A sí mismo la minería sirve para asegurar el sistema contra transacciones fraudulentas o transacciones que gastan la misma cantidad de criptomonedas más de una vez (doble gasto), por lo tanto, si un usuario intenta reutilizar monedas que él mismo ya gastó, la red lo detectará y rechazará la transacción (Santiago, 2016).

9.1.5. Transacción

Las transacciones son el elemento central en una red blockchain, mediante la cual una dirección de la red envía un mensaje a otra dirección de la red. El objetivo final es que se puedan realizar de forma segura transacciones de unidades monetarias o tokens entre usuarios. En este protocolo, una transacción se compone de dos elementos principales:

- Salidas de la transacción. Es la transferencia de fondos. Indica la cantidad de fondos a transferir y el destinatario de los fondos.
- Entradas de la transacción. Son los fondos que se utilizarán para la transacción. Estos fondos deben provenir de una transacción anterior. Por lo tanto en realidad las entradas de una transacción serán referencias a salidas de transacciones anteriores.

Además las transacciones tienen las siguientes características:

- Pueden combinar distintas transacciones de entrada y salida. Es decir una única transacción puede coger fondos de distintas transacciones anteriores y repartirlos de la forma que estime oportuna a distintos destinatarios,
- La suma de importes de entrada debe ser mayor o igual que la suma de importes de salida. Es decir la suma de los fondos de las entradas debe ser igual (o mayor) a la suma de los fondos de las salidas. En la mayoría de los casos un usuario no tendrá transacciones anteriores cuyos fondos sumados den exactamente la cantidad que quiere enviar a la transacción. Lo que se hace es tomar como entradas transacciones anteriores cuyo importe sea superior al necesario, y en la transacción hacer la salida de los fondos que se quieran enviar al destinatario, más otra salida con el importe restante (el cambio) en la que el destinatario es el propio usuario que está haciendo la transacción.
- Comisión. Un usuario, además de las salidas a los destinatarios y a sí mismo (el cambio) puede dejar pendiente un importe. Es decir los importes de las entradas de la transacción son mayores que los importes de salida. Este excedente se denomina comisión y es totalmente voluntario (ya que el usuario que crea la transacción puede establecer las entradas y salidas como prefiera). Esta comisión será para el nodo que procese la transacción, siendo un incentivo para que los diferentes nodos dediquen recursos a procesar las transacciones de los usuarios.

9.1.6. Bloque

Se trata de un conjunto de transacciones que los mineros agrupan para poder resolver el reto. Los mineros intentan genera un bloque con una frecuencia fija y que varía según el tipo de Blockchain. Lo importante es que aquel minero que consiga el reto, además de obtener una recompensa por ser el ganador, incluirá

el nuevo bloque generado, en la cadena de bloques y en este punto comienzan de nuevo a minar el siguiente bloque.

9.1.6.1. Estructura de un Bloque

Un bloque es una estructura de datos contenedor, que agrupa las transacciones para su inclusión en la cadena de bloques. El bloque se compone de una cabecera, que contiene metadatos, seguido por una larga lista de operaciones que componen la mayor parte de su tamaño.

9.1.6.2. Cabecera de Bloque

La cabecera del bloque se compone de tres conjuntos de metadatos de bloque. En primer lugar, hay una referencia a un hash del bloque anterior, que conecta este bloque al bloque anterior en la cadena de bloques; el segundo conjunto de metadatos están relacionados con la competencia en la minería; la tercera pieza de metadatos es la raíz del árbol merkle, una estructura de datos utilizada para resumir, de manera eficiente, todas las transacciones en el bloque.

9.1.6.3. Identificadores de Bloque: Hash de Cabecera de Bloque y Altura de Bloque

El identificador primario de un bloque es su hash criptográfico, que es una huella digital. Un bloque se puede identificar de dos maneras: haciendo referencia al hash de bloque o haciendo referencia a la altura del bloque. Cada bloque posterior, que se añade "encima" de ese primer bloque, está en una posición "superior" en la cadena de bloques. Cada nodo identifica dinámicamente la posición de un bloque (altura) en la cadena de bloques.

9.1.6.4. El Bloque Génesis

El primer bloque en la cadena de bloques se llama el bloque génesis, siendo creado en 2009. Es el ancestro común de todos los bloques en la cadena de bloques (Bitcoin). Cada nodo siempre comienza con una cadena de bloques de al menos un bloque. Cada nodo siempre "sabe" el hash y estructura del bloque génesis, la fecha fija en que fue creado, e incluso la única transacción contenida en él. Por lo tanto, cada nodo tiene el punto de partida para la cadena de bloques, una "raíz" segura desde la que construir una cadena de bloques de confianza.

9.1.6.5. Enlazando Bloques en la Cadena de Bloques

Los nodos completos mantienen una copia local de la cadena de bloques, comenzando en el bloque génesis. La copia local de la cadena de bloques se actualiza constantemente, a medida que se encuentran y se utilizan nuevos bloques para extender la cadena. A medida que un nodo recibe bloques entrantes desde la red, validará estos bloques y luego los enlazará a la cadena de bloques existente. Para establecer un enlace, un nodo examinará la cabecera del bloque entrante buscando el "hash del bloque anterior."

9.2. Funcionamiento de la Blockchain

Según lo descrito en párrafos anteriores la tecnología blockchain se basa en tres fundamentos:

- El registro compartido de las transacciones,
- El consenso para verificar las transacciones realizadas,
- Criptografía como fundamento de todo.

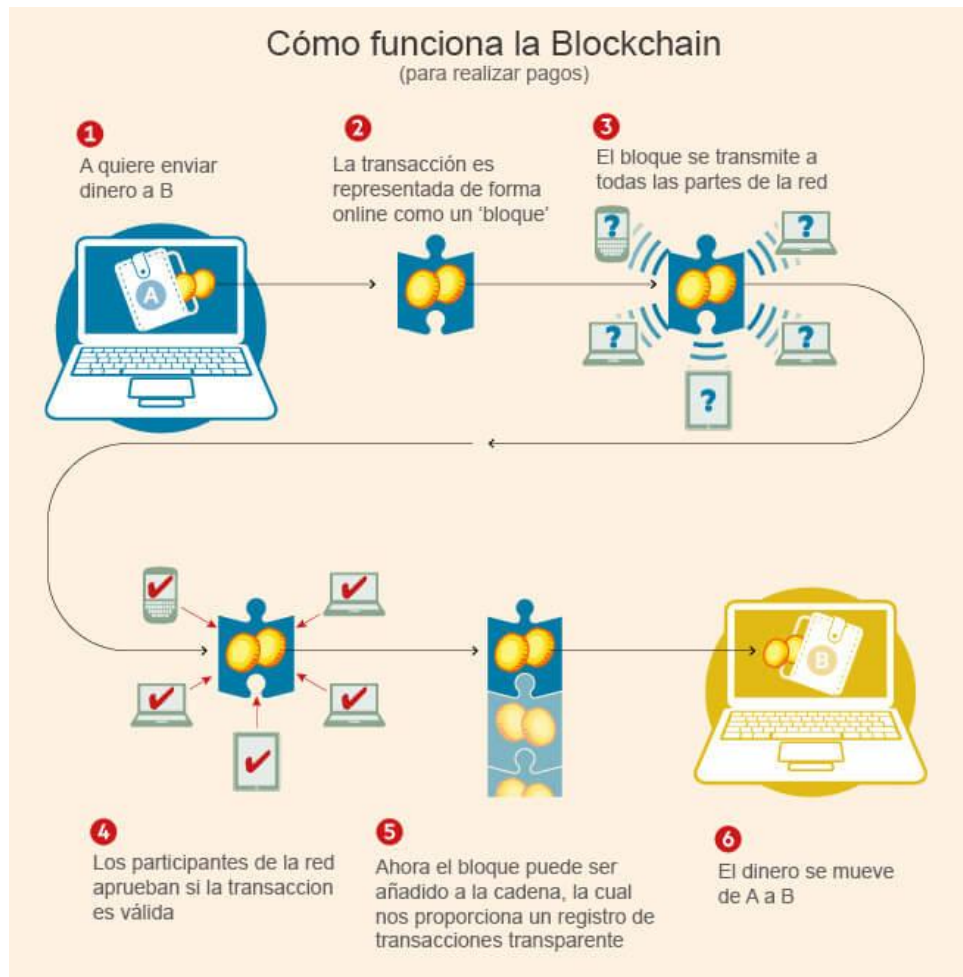


Ilustración N°1. Funcionamiento de blockchain. Fuente: miethereum.com

Imaginemos que “A” usuario de una red blockchain, dese enviar cierta cantidad X de criptomoneda a otro usuario de la red “B”. Los usuarios A y B deben utilizar el software correspondiente para acceder correctamente a la red blockchain en específico. Luego deben obtener las claves criptográficas que servirán para firmar y descryptar los mensajes enviados por la red. Una vez cumplidos estos requerimientos se deberán seguir los siguientes pasos (Porxas & Conejero, 2018):

1. “A” propondrá una transacción al resto de los nodos, indicando que X criptomonedas registrados en su cuenta pasen a ser propiedad de “B” y

- sean eliminados de la suya. El mensaje de A incluye la cantidad de criptomonedas a transferir y la dirección a la que se transfiere.
2. El mensaje con la transacción indicada es recibida de manera encriptada por los nodos validadores, estos deberán verificar que la proposición de transacción ha sido enviada por el usuario que debe transferir las criptomonedas (A), en segunda instancia se debe verificar que el usuario A dispone de la cantidad a transferir, y finalmente se debe comprobar que el destinatario existe (usuario B).
 3. Si el mensaje de A es correcto, los nodos validadores calcularán su hash. El hash, equiparable a una huella dactilar o elemento específico de cada transacción, permite identificar una transacción de forma individualizada, puesto que se obtiene a partir de su concreto contenido y es único.

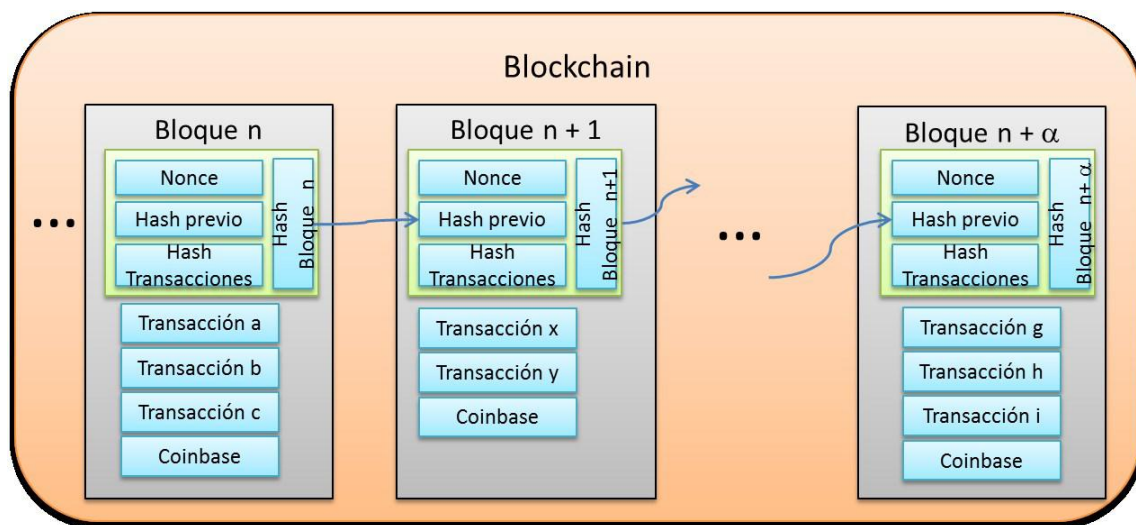


Ilustración N°2. Diagrama verificación de transacciones.

4. La transacción verificada se incluirá en un bloque, es decir, en un paquete de información que contiene las últimas transacciones recibidas y verificadas en un determinado lapso de tiempo. Cada bloque incluye: a. el hash del bloque anterior; b. el hash raíz: el hash resultante de aplicar el algoritmo al conjunto de los hash de todas las transacciones que integran el bloque; c. el

- sello temporal del bloque (día y hora de aprobación); y d. el hash del propio bloque: aplicar la función hash al conjunto de (a, b y c), ver Ilustración N°2.
5. Antes de poder «cerrar el bloque» e incluirlo en la cadena, el nodo validador realiza cálculos para resolver un problema matemático consistente en hallar una combinación numérica (el llamado nonce), que debe colocarse al inicio del hash y que solamente puede ser resuelto mediante prueba y repetición.
 6. La nueva versión del libro registro es remitida a todos los nodos.

9.3. Aplicaciones Descentralizadas Dapps

Dapps, DAO, DAC y DAS son términos abreviados para aplicaciones descentralizadas, organizaciones autónomas descentralizadas, corporaciones autónomas descentralizadas y sociedades autónomas descentralizadas, respectivamente. Esencialmente, este grupo implica una progresión potencial hacia contratos inteligentes cada vez más complejos y automatizados que se vuelven como entidades autónomas, que realizan operaciones preprogramadas y eventualmente autoprogramadas vinculadas a una cadena de bloques. En cierto sentido, toda la ola de protocolos Blockchain 2.0 son DApps, al igual que Blockchain 1.0 (Swan, 2015). La aplicación descentralizada puede ser una App móvil o una aplicación web que interactúa con un contrato inteligente para llevar a cabo su función, que se ejecuta a sí mismo cuando se cumplen las condiciones que fueron programadas en su código (miethereum, 2018).

Una DApp es una aplicación de código abierto de funcionamiento autónomo que almacena criptográficamente sus datos y registros de operaciones en una cadena de bloques pública descentralizada (por ejemplo, a través de un contrato inteligente) para evitar puntos centrales de falla. Utiliza una forma nativa o existente de tokens criptográficos para monetizar la aplicación. Los tokens deben ser necesarios para el uso de la aplicación (Zhang, Schmidt, & Jules White, 2018) .

Para que una aplicación se considere una DApp, debe cumplir con los siguientes criterios:

- La aplicación debe ser 100% código abierto,
- La aplicación debe funcionar de forma autónoma, sin entidad que controle la mayor parte de sus tokens ,
- La aplicación adopta su protocolo en respuesta a las mejores propuestas y todo cambio debe ser decidido por consenso de sus usuarios antes de hacerse efectivas,
- Datos y registros de funcionamiento de la aplicación deben ser almacenados criptográficamente por medio de una blockchain publica, añadiendo transparencia y seguridad como cualidades de la aplicación descentralizada,
- Las operaciones realizadas deben ser almacenadas en bloques por lo que deben ser verificadas mediante protocolo basado en algoritmo prueba de trabajo (PoW) o prueba de participación (PoS),
- Si la DApp funciona según algoritmo criptográfico (PoW o PoS) para la validación de sus bloques, significa que existen mineros o validadores que realizan ese trabajo. Dichos mineros deben ser recompensados por el trabajo realizado mediante criptomonedas o tokens.
- Por validar bloques en la DApp se generan criptomonedas o tokens, con ellas serán recompensados los mineros y además servirá para intercambiar valor dentro de la aplicación.

Tras conocer las características que tiene que tener una DApp para considerarse como tal, pasaremos a diferenciar los distintos tipos de DApps que existen. Esta clasificación de las aplicaciones descentralizadas depende de si poseen su propia blockchain o si bien utilizan la cadena de bloques de otra DApp.

Según este criterio podríamos diferenciar tres tipos de DApps en función del uso que hagan de sus tokens y del blockchain al que estén asociadas:

- **Tipo I.-** Poseen su propia blockchain como es el caso de Bitcoin, Ethereum y Litecoin. Una DApp de tipo I es el equivalente a un sistema operativo de un ordenador.
- **Tipo II.-** Utilizan blockchains de una DApp de tipo I. Estas DApps son protocolos y tienen sus propios tokens necesarios para su funcionamiento, pero no tienen una blockchain propia. Por tanto se realiza una equivalencia entre el token de la DApps tipo I sobre la que funcionan y sus propios tokens. Una DApp del tipo II corresponde al equivalente de un programa con un propósito general (Ej: Word, Excel, etc.).
- **Tipo III.-** Utilizan el protocolo de una aplicación descentralizada tipo II. También son protocolos y utilizan tokens propios que son necesarios para su función, pero no actúan directamente sobre las de tipo I sino que utilizan funciones de tipo II que permiten un desarrollo más rápido y sencillo. El símil de una DApp tipo III es un software especializado, una herramienta que agrega un servicio específico a un programa (Ej: Crystal Ball para Excel).

9.3.1. DAO/DAC

Una DAO/DAC (organización/corporación autónoma descentralizada) es una forma más compleja de una aplicación descentralizada. Para convertirse en una organización más formal, un DApp podría adoptar una funcionalidad más complicada, como una constitución, que delinearía públicamente su gobierno en el blockchain, y un mecanismo para financiar sus operaciones, como la emisión de capital en un crowdfunding. Las DAO / DAC son un concepto derivado de la inteligencia artificial. Aquí, una red descentralizada de agentes autónomos realiza tareas, que se pueden concebir en el modelo de una corporación que funciona sin ninguna intervención humana bajo el control de un conjunto de reglas de negocios (Swan, 2015).

Una DAO es un tipo de organización que es posible gracias a la tecnología blockchain en general y los Smart contracts en concreto. Un 'DAO' es una organización que se ejecuta exclusivamente mediante reglas escritas en contratos inteligentes en un Blockchain (Meunier, 2018). Su diferencia de las empresas convencionales está en que una DAO tiene las reglas de gobierno automatizadas, formalizadas y que se hacen cumplir a través de un algoritmo informático. Básicamente, es un software que permite que los poderes de decisión de la empresa no solo pertenezcan a los directores, sino toda la comunidad que posee tokens (una especie de acciones). La posesión de tokens permite participar en la votación o incluso introducir una propuesta para que el resto la vote. De esta forma, todas las decisiones que se toman están aseguradas por la participación comunitaria en la votación.

9.3.2. DAS

Un concepto que va mas allá de las DAO/DAC comentadas anteriormente es el de DAS (Decentralized Autonomous Societies). Las DAS constituyen asociaciones de conjuntos de DApps, DAOs o DACs que se pueden operar de forma autónoma. La idea de una DAS tiene que ver con la puesta en marcha de sociedades que se rigen de forma automática por uno o varios tipos de contratos, que tienen una forma automática de puesta en funcionamiento a través de mecanismo de crowdsale (evento en línea donde usuarios pueden comprar tokens) normalmente y que son capaces de pagar dividendos a sus accionistas. Adicionalmente las DAS tienen una estructura socioeconómica impregnada de forma automática a su funcionamiento y una estructura política que permite el gobierno de su funcionamiento de forma automática (Lérida & Pérez, 2016).

9.3.3. Lanzamiento de una DApp

El proceso de lanzamiento de una DApp considera la necesidad de realizar los siguientes pasos (Ethereum, 2018):

1. **Creación del ‘White Paper’:** En el mundo de blockchain White Paper (documento Blanco) corresponde al documento, como carta de presentación, que explica las intenciones, los objetivos y los problemas que la DApp desea resolver. Su objetivo es informar a los interesados del potencial de la DApp, su funcionalidad, la distribución de las criptomonedas con las que la DApp operará y el mecanismo de consenso que utilizará. A la vez es usado como herramienta de marketing para seducir a los potenciales clientes.
2. **Establecer una hoja de ruta flexible:** Es necesario explicar los pasos que se van a dar y cómo será dividido en fases o etapas. Es recomendable una programación flexible para que los inversores no pierdan la confianza ante desviaciones o cambios obligados para cumplir con los objetivos planteados.
3. **Realizar una ‘Crowd-sale’ a través de una ICO:** El término ‘Crowd-sale’ hace referencia a la venta masiva de la criptomoneda propia del proyecto, en este caso DApp. Este proceso se lleva a cabo mediante una ‘Oferta Inicial de Moneda’, más conocida como una ICO (Initial Coin Offering). La ICO es un método de financiación a través del cual se ofrece a los inversores una cantidad de esa nueva criptomoneda (token) propia de la DApp a cambio de de otras criptomonedas más conocidas como pueden ser bitcoin o Ether.
4. **Empezar el desarrollo de la DApp:** Una vez recibido los fondos del ‘crowd-sale’ a través de la ICO, es el momento de que el equipo de desarrolladores de la DApp utilice los recursos económicos recibidos a través de la ICO para empezar la creación de la aplicación descentralizada.

9.4. Modelos de Negocio

Tecnologías de la información han transformado y continuarán transformando el paisaje global de los negocios. Modelos de negocio juegan un papel central en esta transformación mediante la vinculación de las tecnologías con las oportunidades de mercado (Najmaei, 2015). Un modelo de negocio describe la lógica de cómo una organización crea, entrega y captura valor (Osterwalder & Pigneur, 2010). Los modelos de negocio son esenciales para determinar cómo las empresas pueden capturar el poder de las tecnologías de la información. El ajuste entre un modelo de negocio y las tecnologías de la información, que son la base de su creación de valor y las actividades de captura, es necesario para que la empresa:

1. Aproveche las necesidades de información de los clientes y las organizaciones en términos de acceso a la información, el intercambio de información y procesamiento de la información como una fuente importante del valor de los clientes,
2. Cree un nuevo valor al cliente mediante el desarrollo de nuevas ofertas y soluciones de mercado de maneras oportunas y rentables,
3. Capture este valor para el cliente para atraer a los clientes a pagar por la oferta y traducir los pagos en beneficios.

En formulaciones estándar, como las "Cinco fuerzas" de Michael Porter, la competencia está determinada principalmente por la estructura de los mercados de entrada y de usuario final. La innovación está ausente en el modelo, y el cambio estructural es raro. Hoy en día, las empresas predominantes luchan por obtener una ventaja duradera. La innovación disruptiva de las empresas de

nueva creación y la entrada por parte de empresas de industrias antes separadas genera una nueva presión competitiva que socava los modelos de negocios existentes (Teece & Linden, 2017).

Las empresas pueden evitar esta barrera con la adopción de las tecnologías que están influyendo en su industria e incorporarlas en sus modelos de negocio en el momento oportuno. Esta estrategia da como resultado modelos de negocio modificados, ajustados o transformados que se basan en parte en los modelos anteriores pero que utilizan ampliamente las nuevas tecnologías para navegar por la empresa de una manera más eficiente. También se puede dar el desarrollo de nuevos modelos de negocio que se basan exclusivamente en las tecnologías de la información. Hay un gran número de posibilidades de modelo de negocio para las empresas que siguen esta estrategia. Esta estrategia conduce a la formación de nuevas industrias y mercados, rompiendo paradigmas y el statu quo como es el caso de iTunes, E-bay, Amazon, Facebook y Wikipedia (Najmaei, 2015).

La competencia ya no es tan empresa contra empresa como lo es ecosistema contra ecosistema. Un ecosistema empresarial contiene una serie de empresas que trabajan juntas (y también compiten) para crear y mantener nuevos mercados y nuevos productos. La coevolución del sistema suele depender del liderazgo tecnológico de una o dos empresas que proporcionan una plataforma en torno a la cual otros miembros del ecosistema, que proporcionan insumos y bienes complementarios, alinean sus inversiones y estrategias. El componente de captura de valor de un modelo de negocio debe encontrar un equilibrio aceptable entre las ganancias para la empresa y la rentabilidad de los socios del ecosistema de la empresa (Teece & Linden, 2017).

La tecnología por sí misma no tiene un solo valor objetivo. El valor económico de una tecnología permanece latente hasta que se comercializa de alguna

manera a través de un modelo de negocio. La misma tecnología comercializada de dos maneras diferentes producirá dos rendimientos diferentes. En algunos casos, una innovación puede emplear con éxito un modelo de negocio que ya es familiar para la firma, mientras que, otras veces, una empresa tendrá un modelo de negocio que puede hacer uso de la tecnología a través de licencias. Sin embargo, en otros casos, una nueva tecnología potencial puede no tener un modelo de negocio obvio, y en tales casos los gerentes de tecnología deben expandir sus perspectivas para encontrar un modelo de negocio adecuado para poder capturar el valor de esa tecnología. De hecho, probablemente sea cierto que una tecnología mediocre aplicada dentro de un gran modelo de negocios puede ser más valiosa que una gran tecnología explotada a través de un modelo de negocios mediocre. A menos que se pueda encontrar un modelo adecuado, estas tecnologías rendirán menos valor a la organización de lo que de otra manera podrían, así como si externos a la organización descubren un modelo de negocio más adecuado para una tecnología determinada, pueden obtener mucho más valor que la empresa que descubrió originalmente la tecnología.

Según (Chesbrough, 2010) sugiere que un modelo de negocio cumpla con las siguientes funciones:

- Articula la propuesta de valor (es decir, el valor creado para los usuarios por una oferta basada en tecnología),
- Identifica un segmento de mercado y especifica el mecanismo de generación de ingresos,
- Define la estructura de la cadena de valor requerida para crear y distribuir la oferta, activos necesarios para apoyar la posición en la cadena,
- Detalla los mecanismos de ingresos mediante los cuales se pagará a la empresa por la oferta,

- Calcula la estructura de costos y el potencial de ganancias (propuesta de valor dada y estructura de cadena de valor),
- Describe la posición de la empresa dentro de la red de valor que une a proveedores y clientes (identificando potenciales complementadores y competidores),
- Formula la estrategia competitiva mediante la cual la empresa innovadora obtendrá y mantendrá la ventaja sobre rivales.

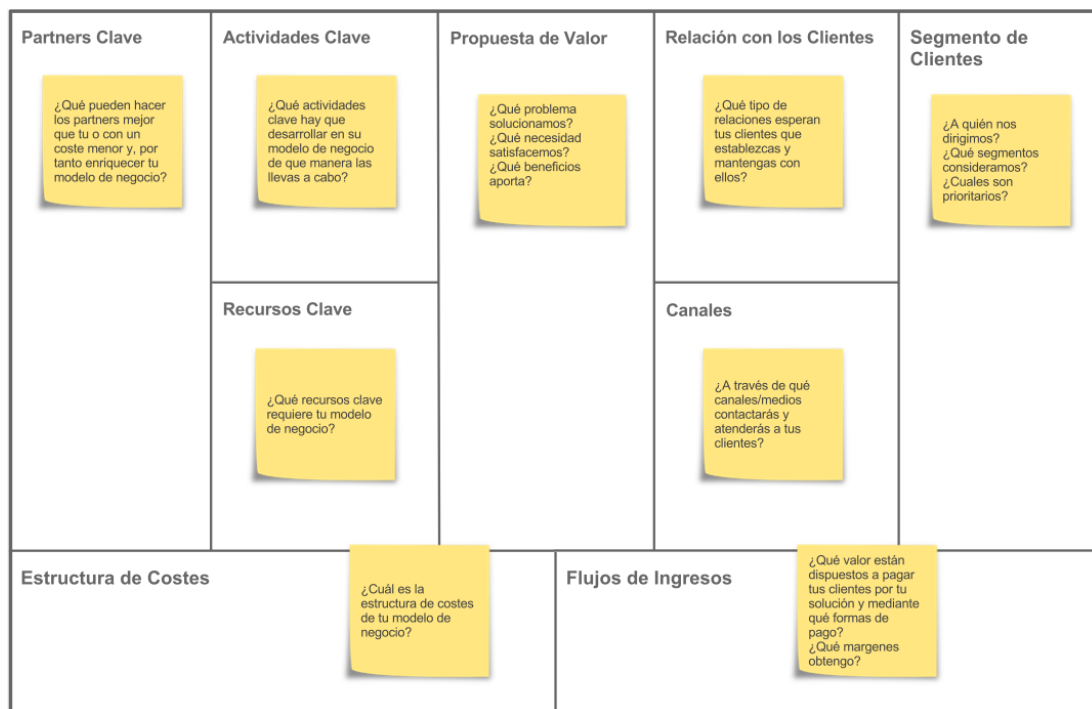


Ilustración N°3. Modelo de Negocios Canvas. Fuente: Macías (2012)

El modelo de negocio de Canvas es un lenguaje compartido para describir, visualizar, evaluar y cambiar los modelos de negocios. Un modelo de negocio puede describirse mejor a través de nueve bloques de construcción básicos que muestran la lógica de cómo una empresa pretende ganar dinero. Los nueve bloques cubren las cuatro áreas principales de un negocio: clientes, oferentes, infraestructura y viabilidad financiera. El modelo de negocio es como un plan

para una estrategia que se implementará a través de estructuras organizativas, procesos y sistemas. (Osterwalder & Pigneur, 2010).

Los nueve bloques del Modelo de Negocio Canvas se detallan a continuación:

1. Segmentos de clientes: Una organización atiende uno o varios segmentos de clientes.
2. Propuestas de valor: Busca resolver los problemas de los clientes y satisfacer sus necesidades.
3. Canales: Las propuestas de valor se entregan a los clientes a través de los canales de comunicación, distribución y ventas.
4. Relaciones del cliente: Las relaciones con los clientes se establecen y se mantienen con cada segmento de clientes.
5. Flujos de ingresos: los flujos de ingresos son el resultado de propuestas de valor que se ofrecen con éxito a los clientes.
6. Recursos clave: Son los activos necesarios para ofrecer y entregar la propuesta de valor.
7. Actividades clave: Actividades centrales generadoras de valor para la empresa.
8. Asociaciones clave: Agentes con los que necesitas trabajar para hacer posible el funcionamiento del modelo de negocio. Algunas actividades se subcontratan y algunos recursos se adquieren fuera de la empresa.
9. Estructura de costos: los elementos del modelo de negocio resultan en la estructura de costos.

9.5. Valor estratégico y Ecosistema Blockchain

Para comprender mejor el valor estratégico general de blockchain y cómo capturarlo se sugiere las siguientes tres perspectivas claves (Carson, Romanelli, Walsh, & Zhumaev, 2018).

1. Blockchain no tiene que ser un intermediario para generar valor, un hecho que fomenta las aplicaciones comerciales autorizadas.
2. El valor a corto plazo de Blockchain consistirá principalmente en reducir costos antes de crear modelos de negocios transformadores.
3. Blockchain está todavía a tres o cinco años de la factibilidad a gran escala, principalmente debido a la dificultad de resolver la paradoja de la "coopetición" para establecer estándares comunes.

Las empresas deben adoptar el siguiente enfoque estructurado en sus estrategias de blockchain:

1. Identifique el valor mediante la evaluación pragmática y escéptica del impacto y la viabilidad a nivel granular, centrándose en abordar los verdaderos puntos de dolor con casos de uso específicos dentro de industrias seleccionadas.
2. Obtener valor al adaptar los enfoques estratégicos de blockchain a su posición en el mercado, teniendo en cuenta medidas como la capacidad de configurar el ecosistema, establecer estándares y abordar las barreras reglamentarias.

Con el enfoque estratégico correcto, las empresas pueden comenzar a extraer valor a corto plazo. Los jugadores dominantes que pueden establecer sus blockchains como las soluciones del mercado deberían hacer grandes apuestas (Carson, Romanelli, Walsh, & Zhumaev, 2018).

Para entender el ecosistema blockchain y poder identificar posibles actores disruptivos y potenciales oportunidades comerciales Riasanow & Burckhardt

(2018), plantean un modelo compuesto por los siguientes actores relevantes: consumidores, proveedores de infraestructura, proveedores de plataforma, proveedores de aplicaciones, proveedores de plataformas de comunicación, minería, proveedores de equipos para minería, proveedores de servicios auxiliares, alianzas, comunidad y servicios de consultoría blockchain.

10. Desarrollo del Tema

En el curso de la revolución tecnológica, los cambios y la innovación continúan llegando rápidamente, y la tecnología blockchain no es una excepción. Para entender su utilidad, potencialidad, oportunidades y desarrollo futuro se debe comprender su ecosistema completo. Según Fredrik Voss, vicepresidente de Blockchain Innovation en Nasdaq, Blockchain es una tecnología que solo funciona en todo su potencial en una red, por lo tanto debe tener un ecosistema completo para que ofrezca el máximo valor a todos sus participantes (Nasdaq, 2016).

A continuación se presenta un análisis del ecosistema Blockchain analizando a sus principales participantes y sus relaciones, con el fin de entender el valor entregado por la tecnología en cada eslabón de la cadena de valor de la industria. De esta manera se puede comprender el impacto generado, oportunidades de innovación, desarrollo de negocios y barreras existentes.

10.1. Análisis Ecosistema Blockchain

Según el diseño de investigación planteado para analizar el ecosistema blockchain y sus impactos en los modelos de negocio se realiza una unión de los modelos Business Model Canvas (Osterwalder & Pigneur, 2010) y el ecosistema blockchain planteado por (Riasanow, Burckhardt, Setzke, Böhm, & Krcmar, 2018), con el fin de obtener una visión holística sobre la tecnología blockchain.

El análisis de los participantes relevantes de la industria se realiza con información estratégica presente en sus sitios WEB, Documento Blanco, y usos de bases de datos Owler y Crunchbase.

10.1.1. Consumidores

En el ecosistema blockchain un consumidor puede necesitar infraestructura, plataformas y DApps, viéndolo desde el punto de vista de un consumidor final, así mismo los proveedores de estas son a la vez clientes de proveedores de servicios de minería, consultores, consorcios o alianzas. Tomándolo desde esta perspectiva en muchos casos un cliente actúa como un prosumidor produciendo un servicio y consumiendo a la vez.

En los siguientes apartados se procede a analizar a cada uno de los participantes del ecosistema blockchain, para posteriormente entender tanto la perspectiva de cliente como de proveedor y el valor agregado a lo largo de la cadena de valor de la industria.

10.1.2. Proveedores de Infraestructura Blockchain

Los Proveedores de infraestructura corresponden a las DApps Tipo I, así como también aplicaciones privadas que poseen su propia blockchain. Ellos son quienes entregan la infraestructura, incluyendo el marco conceptual, la tecnología DLT y las criptomonedas, además permiten la creación de aplicaciones descentralizadas tipo II aportando al crecimiento del ecosistema y su adopción. Algunos de los proveedores más importantes de infraestructura se detallan a continuación:

- Bitcoin: aplicación descentralizada de código abierto; su diseño es público, nadie es dueño o lo controla y todo el mundo puede participar. Usa tecnología peer-to-peer para operar sin una autoridad central o bancos; la gestión de las transacciones y la emisión de bitcoins es llevada a cabo de forma colectiva por la red.

- **Ethereum:** plataforma y lenguaje de programación para crear y publicar aplicaciones distribuidas. Se puede utilizar para codificar, descentralizar, asegurar y comercializar casi cualquier cosa: votación, nombres de dominio, intercambios financieros, financiación colectiva, contratos y acuerdos, propiedad intelectual e incluso propiedad inteligente gracias a la integración de hardware.
- **Ripple:** sistema de pago global en tiempo real que permite a los bancos e instituciones financieras de todo el mundo realizar transacciones directas entre sí sin la necesidad de un corresponsal central.

La mayoría de los proveedores de infraestructura poseen criptomonedas que son la base para efectuar pagos y transacciones de activos. La capitalización total del mercado de criptomonedas es de USD 203.536.241.468 a octubre 2018, en la Tabla N°1 se puede ver el detalle de las principales criptomonedas y su capitalización.




#	Nombre	Símbolo	Precio (USD)	Cap. mercado	Vol. (24h)	Vol. total	Var. (24h)	Var. (7d)
1	 Bitcoin	BTC	6.353,7	110,14B \$	3,75B \$	36,08%	-0,07%	-1,86%
2	 Ethereum	ETH	198,04	20,34B \$	1,34B \$	12,85%	-0,32%	-2,55%
3	 Ripple	XRP	0,44913	17,90B \$	274,35M \$	2,64%	+1,07%	+0,37%

Tabla N°1. Capitalización de las principales criptomonedas. Fuente: Investing.com

Para el análisis de negocio se seleccionaron los proveedores que poseen las criptomonedas con mayor capitalización bursátil. En el Cuadro N°4 se puede apreciar que la propuesta de valor que comparten estas compañías es el de pagos y transferencias descentralizadas que otorgan una mayor agilidad al proceso y una reducción de costos al eliminar las fricciones asignadas por terceros. No obstante Ethereum se destaca en este sentido de Bitcoin y Ripple, si bien inicialmente el proyecto comenzó con una preventa de Ether (su

propia criptomoneda ETH), posee como propuesta la entrega de un lenguaje de programación para la creación de aplicaciones en base a sus contratos inteligentes. En tanto, Ripple se diferencia de Bitcoin y Ethereum al apuntar a un segmento objetivo claro como lo son las instituciones financieras, entregando productos y servicios asociados a generar una red de bancos global con claras relaciones de venta.

Los proveedores de Infraestructura basan sus actividades en investigación y desarrollo para entregar seguridad y descentralización a través de sus mecanismos de consenso, si bien son aplicaciones de código abierto deben realizar el esfuerzo de reclutar el talento necesario mediante socios estratégicos para llevarlo a cabo, acudiendo a comunidades de desarrolladores, proveedores de minería, software y hardware.

Otro punto donde Ripple se diferencia del resto es que no requiere operaciones mineras para aprobar las transacciones, utilizando protocolo de consenso (acuerdo distribuido) donde varias partes verifican tomando la opinión de la mayoría para lograr el acuerdo. De esta manera Ripple es más eficiente en términos de tiempo de proceso de la transacción. Para el caso de pagos transfronterizos Ripple toma 4 segundos en comparación con: Ethereum 2 minutos, Bitcoin 1 hora y Sistemas tradicionales 3-5 días.

Su forma de financiarse también marca un contraste, mientras Bitcoin y Ethereum son entidades sin fines de lucro y en general se financian vía donaciones, Ripple lo hace a través de la venta de licencias y uso de software marcando claramente los diferentes propósitos, mientras Ripple pretende desarrollar red global de pagos por medio del sistema financiero, Bitcoin y Ethereum buscan la descentralización, desarrollo y adopción de la tecnología.

Áreas	Ítem	Empresa		
		Bitcoin	Ethereum	Ripple
Oferta	Propuesta de Valor	Pagos y transferencias seguras, baja o ninguna comisión, sistema descentralizado.	Contratos inteligentes, programación para el fácil desarrollo de aplicaciones blockchain,	Red global de pagos, liquidez, pagos y transferencias instantáneas sin fricción a menor costo.
	Flujo de Ingresos	Donaciones, Bajas tarifas de transacción.	Donaciones,	Instalación Software, Licencia anual XCurrent, Inversores.
Financiera	Estructura de Costos	IT, mantenimiento WEB, plataforma, proyectos, I+D, eventos.	I+D, sistemas, Desarrollo de software, Desarrolladores, Mantenimiento plataforma, Infraestructura y operación.	I+D, TI, operación, mantenimiento infraestructura, personal, administración y ventas.
	Segmento de Cliente	Individual, desarrolladores, negocios, comunidades criptomonedas.	Individuales, desarrolladores, negocios, , comunidades criptomonedas, Comunidad IT,	Bancos, sistema financiero.
Cliente	Canales	Internet, plataformas, redes sociales, red distribuida, sitio web, Wallet Pagos, Proveedores de Servicio.	Sitio web, redes sociales, internet, API, Wiki, Press	Sitio Web, plataforma, internet, redes sociales, sistema de pagos, aplicaciones, transferencias e inversiones.
	Relación con Clientes	Virtual, online, digital, Comunidad, colaboración, Confianza, transparencia.	Comunidad, democratización de inversiones, asesorías, transparencia, diseño y emisión de criptomonedas propias, proyectos con confianza colectiva,	Virtual, online, asistencia personal, Comunidad, inversiones, socios, servicios automatizados, proveedores de pago, asesorías, intercambio de activos digitales,
	Actividades Claves	Desarrollo de software, Procesos seguros, Promover uso y adopción.	I+D, desarrollo de software, seguridad, promover adopción, comunidad,	I+D, promover adopción, desarrollo de ecosistema, plataforma, marketing, comunicación, soporte clientes.
Infraestructura	Recursos Claves	Mineros, plataforma, Comunidad desarrolladores de sistema de código abierto. Comunidad blockchain.	Plataforma blockchain, Ethereum Wallet, Ether, comunidad, Licencias de código abierto.	Plataforma Ripple, desarrolladores, software, hardware, infraestructura,
	Asociaciones Claves	Fundación Bitcoin, Linux Mineros Bitcoin, Comunidad de desarrolladores, Wallets Licencia MIT, Donantes, Comercio.	Comunidad blockchain, Desarrolladores, Donantes, Wallets	Bancos, sistema financiero, comunidad de desarrolladores,

Cuadro N°4. Análisis modelo de negocio de proveedores de infraestructura blockchain.

10.1.3. Proveedores de Plataforma Blockchain

Los proveedores de plataforma proporcionan las DApps tipo II que utilizan la infraestructura (blockchain) de las DApps tipo I para la creación de protocolos, a su vez también existen proveedores de plataformas privadas. Ofrecen la base técnica y herramientas de desarrollo de blockchain, incluyendo conjuntos de API (Interfaz de programación de aplicaciones), contratos inteligentes y tokens permitiéndole a desarrolladores crear aplicaciones descentralizadas. Algunos importantes proveedores de plataforma son:

- **Etherparty:** entrega herramientas simples para crear aplicaciones basadas en blockchain fáciles de usar para la creación, uso y administración de contratos inteligentes.
- **Omni Layer:** Es una capa de software construida sobre la blockchain de Bitcoin, permitiendo la creación de tokens para representar monedas o activos personalizados, blockchain basado en crowdfunding y comercio peer-to-peer.
- **Multichain:** apoya a las organizaciones a crear e implementar aplicaciones de blockchain con un desarrolla amigable, personalizable y seguridad flexible.

Los proveedores de plataforma tienen como propuesta de valor la entrega de herramientas para crear tokens y aplicaciones. Sus principales clientes son empresarios, emprendedores y cadenas de suministro atendidos mediante sus sitios web, plataformas, blogs y redes sociales, entregando servicios de creación, desarrollo de aplicaciones y asistencia. Además, con el interés empresarial por implantar 'blockchain' y las dificultades reales para hacerlo están provocando que varias compañías tecnológicas ya ofrezcan servicios de

Blockchain como un Servicio (BaaS) para las empresas que prefieren externalizar el desarrollo de soluciones 'blockchain'. De esta manera su flujo de ingresos está constituido por el cobro de tarifas de transacción y la ventas por servicios BaaS.

Áreas	Ítem	Empresa		
		Etherparty	Omni Layer	Multichain
Oferta	Propuesta de Valor	Creación de acuerdos entre personas.	Crear y comercializar activos y monedas digitales.	Implementación de aplicaciones blockchain
Financiera	Flujo de Ingresos	Blockchain como servicio, Tarifas comerciales	Tarifas comerciales	Blockchain como servicio, Licencias comerciales
	Estructura de Costos	Desarrollo de software, IT Operación y mantenimiento, I&D, hosting	Desarrollo de software, IT Operación y mantenimiento, I&D, hosting	Desarrollo de software, IT Operación y mantenimiento, I&D, hosting
Cliente	Segmento de Cliente	Empresarios y dueños de negocio, Empresas de logística, cadena de suministro.	Emprendedores, Empresarios, Negocios.	Negocios, empresarios, empresas establecidas.
	Canales	Plataforma, sitio web, redes sociales, Internet. Blog, Bitcointalk, Github, Reddit.	Plataforma, sitio web, redes sociales, API, Internet, Github, Reddit.	Plataforma, sitio web, redes sociales, API, Internet, Github, Reddit.
	Relación con Clientes	Creación de aplicaciones, Contratos inteligentes, Comunidad, Co-creación Asistencia.	Creación de token, Crowdfunding, Comercio peer-to-peer. Co-creación, Asistencia	Construcción de blockchain público, privado, Aplicaciones, Despliegue, Activos, Flujo de datos, Permisos, asistencia, seguridad
Infraestructura	Actividades Claves	Desarrollo de Aplicaciones, plataformas, seguridad.	Desarrollo de Plataforma, Wallet, Protocolo, I&D.	I&D, Plataformas, protocolos.
	Recursos Claves	Software, hardware, desarrolladores especializados, Crowdfunding.	Software, hardware, desarrolladores especializados, Crowdfunding.	Software, hardware, desarrolladores especializados,
	Asociaciones Claves	RSK, Ethereum, Blockchain UBC, Desarrolladores, Coin Payment, Comunidad.	Ambisafe, Holy Transaction, Bitcoin, Desarrolladores, Comunidad	Consultorías TI, Accenture, Blockchain Mate, Proveedores de productos, Election Explorer, New Banking.

Cuadro N°5. Análisis modelo de negocio proveedores de plataforma blockchain.

Las actividades claves de este tipo de proveedor se concentran el desarrollo plataformas y protocolos seguros para aplicaciones con un fuerte esfuerzo en I&D, para ello requieren de software, hardware, personal altamente capacitado,

asociaciones con proveedores de infraestructura y comunidades de desarrolladores, quienes son recompensados por aportar al desarrollo y detección de fallas críticas, de esta manera estas actividades claves son las que conforman su estructura de costos (Equipos, operación y mantenimiento de TI, I&D).

10.1.4. Proveedores de Aplicaciones Blockchain

Los proveedores de aplicaciones son quienes ofrecen DApps tipo III y aplicaciones privadas. Son quienes conectan al usuario final con blockchain por medio de aplicaciones e internet, entregando soluciones en todos los ámbitos de la economía, preocupándose por entregar un funcionamiento seguro, gestionando recursos y riesgos. En definitiva son quienes crean y aumentan el mercado de blockchain y las criptomonedas a través de los tokens generados por las ICOs. Con el fin de analizar a los proveedores de aplicaciones y su relación con el usuario final se revisan los modelos de negocio de algunas aplicaciones importantes y en la actualidad son:

- **La'zooz:** Una plataforma de transporte descentralizado propiedad de la comunidad y que utiliza el espacio no utilizado de los vehículos para crear una variedad de soluciones de transporte inteligentes. Mediante el uso de la tecnología de criptomoneda, La`Zooz funciona con un mecanismo de recompensa Fair Share (Participación Justa) para desarrolladores, usuarios y patrocinadores.
- **Sun Exchange:** A través de la aplicación cualquiera puede usar la energía solar y comenzar a crear riqueza alimentada por la luz solar. Otorga ingresos por alquileres en cualquier lugar del mundo a través de un sistema de pago basado en blockchain. Los proyectos solares están asegurados

contra incendios, daños y robos. Sus células solares generarán riqueza a partir de la luz solar durante 20 años. Una fuente sin esfuerzo de ingresos sostenibles.

- **ODM:** La plataforma conecta a estudiantes, educadores y proveedores de servicios para desarrollar y participar en programas educativos personales y grupales. Estudiantes y otros compradores de educación pueden investigar y encontrar fácilmente el plan de estudios perfecto de educadores de todo el mundo. Para los educadores, aumenta su visibilidad entre todos los compradores de educación, genera comentarios en tiempo real sobre los programas y paga incentivos para el desarrollo de programas relevantes.

Como se puede apreciar en el Cuadro N°6, este tipo de proveedores tienen como propuesta de valor entregar un servicio colaborativo a la comunidad, descentralizado, eliminando las estructuras de costo elevadas por una administración ineficiente. Estos proveedores pueden apuntar sus propuestas a prácticamente todas las industrias repercutiendo en la forma en que se realizan los negocios en la actualidad, sacando al tercero del medio. Sus canales de clientes se establecen básicamente por medio de aplicaciones, internet, blog y redes sociales. Así, tenemos el caso de La'zooz que puede ser un potencial competidor de UBER modificando su modelo de negocio al distribuir los beneficios con la comunidad, en tanto Sun Exchange se puede transformar en un real competidor de proveedores de energía, entregándola de forma colaborativa y respetando el medio ambiente. Por otro lado tenemos a ODEM como comunidad colaborativa que busca reducir el costo y mejorar la accesibilidad al sistema de educación superior con programas que pueden ser personalizados, si bien puede transformarse en competencia para algunas compañías educativas busca la cooperación con distintas universidades fomentando el fortalecimiento de su ecosistema. Los flujos de ingresos para

este tipo de proveedor están compuestos principalmente por tarifas asociadas al uso y venta de tokens por medio de las ICOs.

Áreas	Ítem	Empresa		
		La'zooz	Sunexchange	ODEM
Oferta	Propuesta de Valor	Transporte colaborativo mediante plataforma descentralizada.	Energía limpia con propiedad descentralizada.	Mercado educativo a pedido mediante contratos inteligentes.
	Flujo de Ingresos	Tarifas por uso, ICOs	Tarifas por uso, ICOs	Tarifas por uso, ICOs
Financiera	Estructura de Costos	Desarrolladores, Miembros, Plataforma, Operación y Mantenimiento TI, Patrocinadores.	Plataforma, operación y mantenimiento, Servicios de terceros, desarrolladores, patrocinadores, usuarios.	Plataforma, operación y mantenimiento TI, desarrolladores, patrocinadores, usuarios.
	Segmento de Cliente	Usuarios y proveedores de de transporte, inversores.	Inversores, usuarios de energía.	Estudiantes, profesores, inversores, ejecutivos, compañías educativas, departamentos de RRHH.
Cliente	Canales	Sitio web, plataforma, internet, medios sociales, blog.	Sitio web, plataforma, internet, medios sociales.	Sitio web, plataforma, internet, medios sociales.
	Relación con Clientes	Colaboración, descentralizada, transporte inteligente, experiencia de viaje.	Medio ambiente, mercado, contratos, arriendo, rentabilidad.	Servicios educativos, facilitadores, desarrollo, oportunidades, redes eficientes, contratos, soporte, asistencia.
Infraestructura	Actividades Claves	TI, operación y mantenimiento aplicación, seguridad, marketing.	Evaluación y ejecución de proyectos solares, operación y mantenimiento aplicación, seguridad, Marketing.	Educación, desarrollo y entrega de contenido, incremento de nuevos mercados, incremento de nuevos negocios, construcción de redes eficiente, TI.
	Recursos Claves	Minería de camino, desarrolladores, TI, software, hardware, algoritmos de ruta y retribución de participación justa.	TI, desarrolladores, celdas solares, cartera solar, instalaciones solares, operación y mantenimiento de instalaciones.	TI, desarrolladores y arquitectos de sistemas, aplicación, Inversores, filántropos, sponsor de educación y contenido, educadores.
	Asociaciones Claves	Comunidad, entidades públicas, proveedores de blockchain, Omni, Etehreum, Inversores iniciales, usuarios iniciales.	Inversores iniciales, Empresas de ingeniería, adquisiciones y construcción, proveedores de infraestructura solar, Ethereum, Bitcoin, Power Hive, Barclays Bank.	Patrocinadores, Ethereum, comunidad educativa, comunidad estudiantil, inversores iniciales, usuarios iniciales.

Cuadro N°6. Análisis de modelo de negocio de proveedores de aplicaciones blockchain.

En cuanto su infraestructura, las actividades claves están relacionados a infraestructura TI, seguridad, operación y mantenimiento de aplicaciones y actividades relacionadas a las industrias donde operan. Sus recursos claves son los proveedores de su industria en particular, TI, software, hardware, especialistas en desarrollo y arquitectura, proveedores de plataforma blockchain y comunidades claves. La utilización de los recursos mencionados traza la estructura de costos de estos proveedores del ecosistema blockchain.

Además de las DApps, como las analizadas, también existen aplicaciones privadas, las que obviamente no son descentralizadas y están destinadas a mejorar procesos dentro de una organización como es el caso de los sistema de transferencias del sistema financiero, sistemas de votación, trazabilidad de la cadena de suministro. De esta manera se puede entender que las DApps están asociadas a la colaboración y beneficio de la sociedad en contraste con las aplicaciones blockchain privadas que están relacionadas a la mejora de procesos de las industrias con una clara visión al beneficio empresarial.

10.1.5. Proveedores de Plataforma Comunitaria Basadas en Tokens

Los proveedores de plataformas comunitarias poseen sistemas de recompensas en token para recompensar contenido previa evaluación. Los token son representados mediante contratos inteligentes y distribuidos o destruidos según las reglas definidas. Algunos de estos actores son:

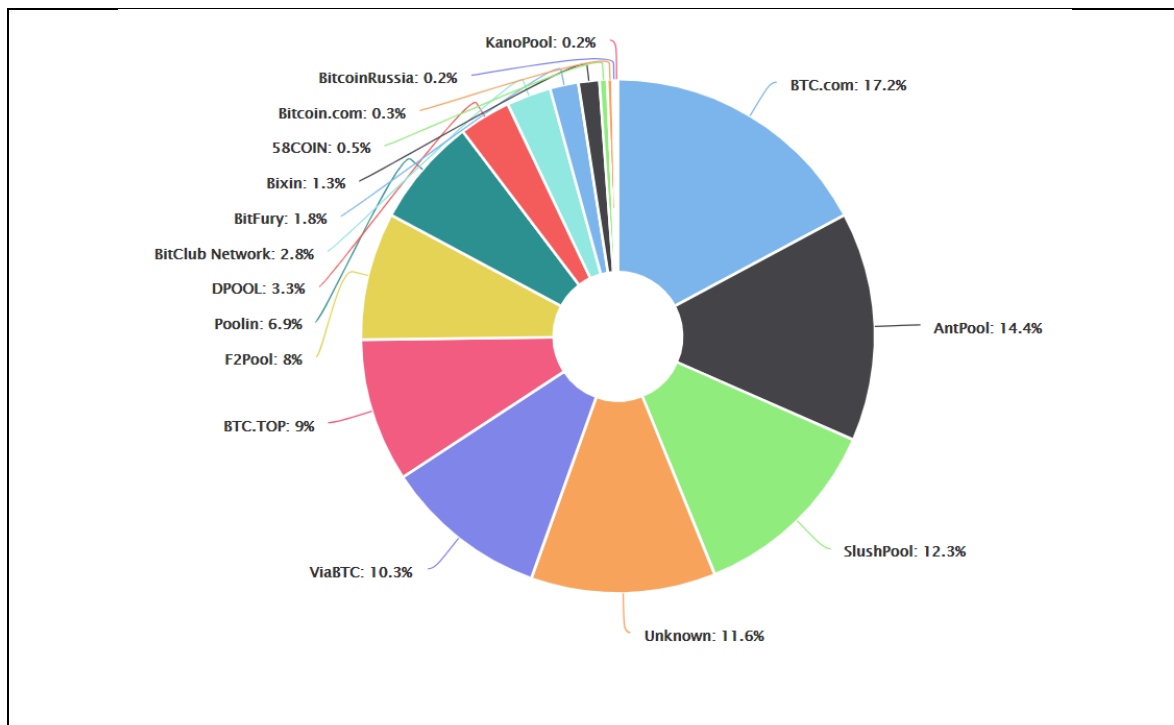
QunQun: plataforma de comunidad de incentivos, donde las personas pueden crear sus propias comunidades temáticas, una especie de Twitter autónomo e independiente entre sí, sin ningún tipo de programación e implementación. Las personas obtienen recompensas QunQun (token) al ejecutar su propia comunidad o al participar en otras contribuciones.

SocialX: plataforma de medios sociales impulsada por la comunidad que permite a los usuarios publicar contenido, fotos y videos. Es un símil de Facebook e Instagram, sin embargo su diferencia consiste en ser una plataforma blockchain descentralizada donde todos pueden ganar recompensas de token SOCX.

La propuesta de valor de los proveedores de plataforma comunitaria es generar comunidades que compartan sus contenidos y sean recompensadas por publicarlo, generando un mercado comunitario. Sus modelos de negocio son similares a los descritos para los proveedores de aplicaciones blockchain.

10.1.6. Minería

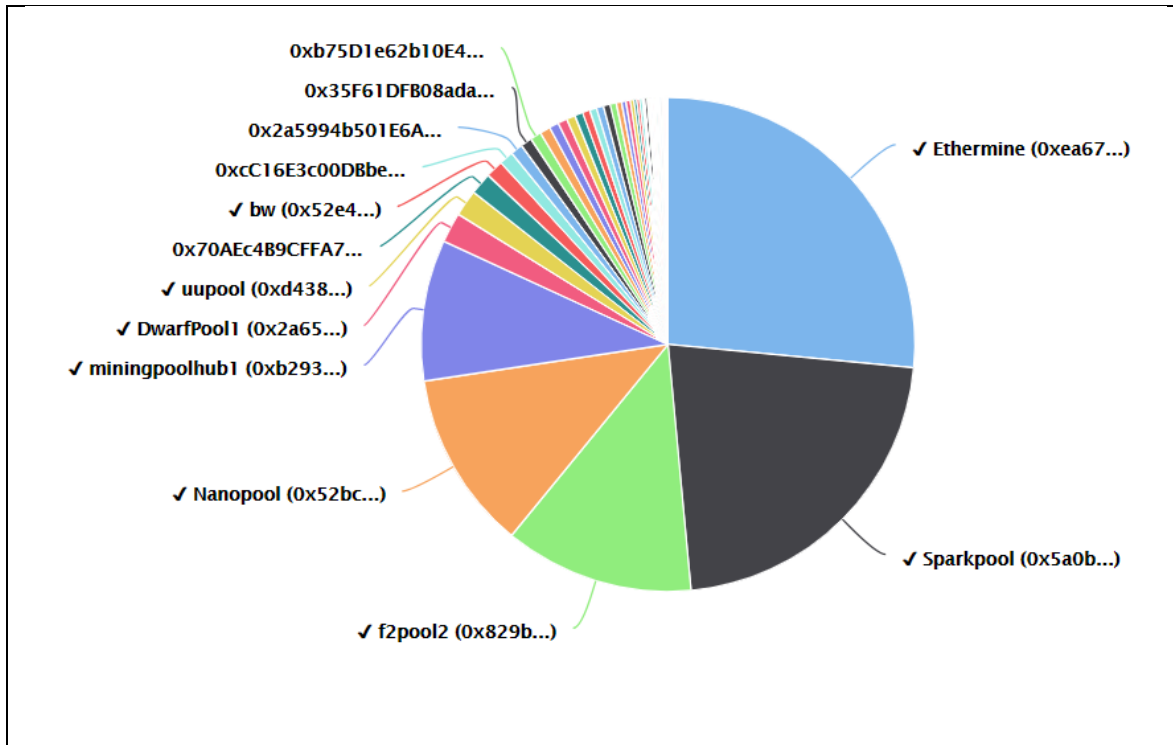
El objetivo principal de la minería es mantener la red estable mediante el consenso general. Los mineros son los responsables de verificar las transacciones dentro de la blockchain resolviendo las pruebas propuestas, utilizando software y hardware especializado. El primero en resolver el problema es recompensado con la respectivas criptomoneda asociada a la blockchain. Existe baja probabilidad de éxito minando bloques por cuenta propia, por ello existen las “mining pool” (piscina minera) que son agrupaciones de mineros que unen sus recursos para aumentar las probabilidades de éxito y dividen las recompensas. Los principales mining pool en la actualidad para Bitcoin son BTC.com, AntPool y SlushPool.



Gráficos N°1. Distribución de los principales Mining Pool de Bitcoin.

Fuente: <https://www.blockchain.com/es/pools>

Mientras que para Ethereum las principales son Ethermine, SparkPool y F2Pool2.



Gráficos N°2. Distribución de los principales Mining Pool de Ethereum.

Fuente: <https://www.etherchain.org/charts/topMiners>

El objetivo del negocio de la minería de transacciones es otorgar seguridad y estabilidad a la red mientras se obtienen ganancias por medio de las recompensas obtenidas.

La infraestructura requerida para el desarrollo del negocio consiste en servidores, software, hardware, energía, generación de comunidades de mineros, desarrollo de tecnología a los nuevos requerimientos de minado. Los clientes de los mining pool son las distintas criptomonedas y sus DApps asociadas.

Es indispensable que la estructura del minado de transacciones este compuesto por un gran número de oferentes, ya que de esta manera se consiguen los

objetivos de la tecnología blockchain, que es descentralizar y otorgar seguridad en redes sin confianza.

A continuación se presenta un análisis del modelo de negocio de forma genérica para este tipo de participantes del ecosistema blockchain.

Modelo de Negocios Canvas Mining Pool				
* Socios Claves	* Actividades Claves	* Propuesta de Valor	* Relaciones con Clientes	* Segmentos de Clientes
Mineros, Proveedores de almacén de datos, Servidores	Comunidad, Seguridad, Desarrollo de software, Operaciones,	Proporcionar funcionalidades, seguridad y estabilidad, un servicio excelente y ganancias para los clientes.	Virtual Online Seguridad, Transparencia	Criptomonedas (Bitcoin, Ethereum, Litcoin, etc.), DApps.
	Recursos Claves Energía Hardware, Software Servidores, Infraestructura.		*Canales Internet, Sitio Web, Proveedor de Servicio	
* Estructura de Costos		* Fuentes de Ingresos		
Costos de energía, Costos de tarifas, Comisiones, Infraestructura, Seguridad.		Recompensas por minado de bloques.		

Cuadro N°7. Análisis de modelo de negocio de las Mining Pool.

10.1.7. Proveedores de Equipos y Soluciones Mineras

Los proveedores de equipos y soluciones de minería entregan el software y hardware necesario para ejecutar el proceso minero, esto incluye la venta de equipos, procesadores, servicio de mantenimiento y reparación. Los equipos

más utilizados son los GPUs (Unidades de procesamiento gráfico) y ASIC (circuito Integrado para aplicaciones específicas).

Además los proveedores entregan servicio de minería como un servicio (MaaS), para quienes pretendan explotar criptomonedas sin poseer ningún equipo, ofreciendo capacidad de extracción en línea. Otro servicio ofrecido son las consultoría para configurar y operar granjas mineras.

Los principales proveedores de equipamiento son Bitmain Technologies, Giga Watt, CloudHashing.

- Bitmain: Fabricante de hardware de minería Bitcoin y otros servicios relacionados. La compañía también opera el grupo de minería de Bitcoin más grande y el segundo más grande del mundo en términos de potencia informática, BTC.com y Antpool. Bitmain es compatible con una amplia gama de plataformas y startups de blockchain, y participa activamente en el desarrollo de la industria y la comunidad.
- Giga Watt: El primer proveedor de soluciones de minería de servicio completo del mundo. Servicios de minería llave en mano o paquetes personalizados. Presentan una gama completa de servicios de minería desde la venta, mantenimiento y reparación de equipos hasta el servicio privado de cadenas de bloques.
- CloudHashing: empresa de minería de Bitcoin como servicio que ofrece contratos de minería en la nube, para facilitar que cualquiera pueda invertir en la minería. La plataforma de minería de bitcoin basada en la nube contiene centros de datos en todo el mundo.

10.1.8. Proveedores de Servicios Auxiliares

Los proveedores de servicios auxiliares están comprometidos con el desarrollo del ecosistema blockchain, prestando servicios de asistencia, estudios, asesorías técnicas, capacitaciones abiertas, talleres y cursos personalizados a nivel mundial. Los principales proveedores son:

- **SettleMint:** Busca acelerar el camino para aprovechar los beneficios de la tecnología blockchain, entregando servicios que permiten mejorar la eficiencia, extender productos actuales a nuevos segmentos de clientes, modificar completamente un modelo de negocio. Además tienen como propósito informar, educar y capacitar a todos los que quieran comprender y aprender sobre la tecnología Blockchain.
- **BTC Media:** la compañía de medios de bitcoin y blockchain más grande del mundo, distribuyen la información, educación e investigación que están construyendo los sistemas financieros del futuro. Sus clientes incluyen a todos, desde startups de tecnología hasta gigantes financieros de Fortune 500. Su visión es que el dinero se mueva más rápido, más barato y más conveniente alrededor del mundo. BTC Media mantiene al mundo informado a través de productos y servicios que incluyen Bitcoin Magazine, yBitcoin y The Distributed Ledger.
- **Sweetbridge:** conecta a personas con recursos subutilizados como activos, habilidades, propiedad intelectual y redes de confianza, a las empresas que desean mejorar el rendimiento, permitiendo a todos los participantes (organizaciones e individuos) aportar resultados que solucionen problemas disruptivos, mejorar la liquidez de los activos, y crear valor mutuamente compartido.

La propuesta de valor entregada por este tipo de participantes del ecosistema blockchain, tiene relación con el desarrollo de la tecnología, las comunidades, asesorías y la búsqueda de la eficiencia de las actividades claves del negocio.

10.1.9. Alianzas Blockchain

Actualmente existen asociaciones fundadas para unificar esfuerzos para crear oportunidades de crecimiento que beneficien a todos los participantes a través de la cadena de valor de la industria. Las alianzas abordan los requisitos de implementación generando innovación, integración global de sistemas, educación y certificación de profesionales, marco regulatorio de la tecnología y estructura de mercados. A continuación se presentan alianzas relevantes en el ecosistema blockchain:

- Hyperledger: esfuerzo de colaboración de código abierto creado para avanzar en las tecnologías de cadena de bloques de la industria. Colaboración global, organizada por la Fundación Linux, que incluye líderes en finanzas, banca, Internet de las cosas, cadenas de suministro, fabricación y tecnología.
- R3: empresa de software de blockchain empresarial que trabaja con un amplio ecosistema de más de 200 miembros y socios en múltiples industrias, tanto del sector público como privado. Poseen su propia plataforma de cadena de bloques de código abierto y también una versión comercial para empresas, Corda y Corda Enterprise respectivamente.
- Enterprise Ethereum: conecta a las empresas de Fortune 500, empresas emergentes, académicos y proveedores de tecnología con expertos en la materia de Ethereum. Tiene como fin definir el software de nivel empresarial

capaz de manejar las aplicaciones más complejas y exigentes a la velocidad de los negocios, por medio de contratos inteligentes Ethereum.

La propuesta de valor de estas alianzas está relacionada con la innovación, regulación, educación y generación de adopción de la tecnología para el beneficio de la industria, agilizando procesos y restricciones legales.

10.1.10. Comunidad Blockchain

Entidades compuestas por profesionales, desarrolladores y aficionado, y son cruciales para impulsar la tecnología de blockchain. Estas comunidades discuten aplicaciones, nuevas criptomonedas, ventas masivas, representando y defendiendo intereses comunes. Algunas de estas comunidades son:

- **Blockchain Community:** comunidad voluntaria sin fronteras de empresarios, servicios, expertos y entusiastas de blockchain. Su misión declara, establecimiento de relaciones personales y de negocios cercanas entre los miembros de la comunidad. Establecimiento de nuevas colaboraciones prospectivas, intercambio de ideas, tecnologías y experiencias. Buscando el beneficio de cada miembro de la comunidad.
- **IEEE:** organización profesional técnica dedicada al avance de la tecnología en beneficio de la humanidad. Ayuda a mantenerse al tanto de los desarrollos en la tecnología blockchain. Participar en la comunidad garantiza la recepción de noticias y anuncios de conferencias, educación, publicaciones, estándares y otras oportunidades para tener conocimiento del progreso de la investigación, el desarrollo y la planificación.

Estas instituciones buscan el desarrollo de la tecnología, compartiendo ideas y experiencia para el beneficio de la comunidad

10.1.11. Servicios de Asesoramiento Blockchain

Estas organizaciones apoyan y orientan con su conocimiento y experiencia a las empresas que utilizan o desean incluir la tecnología en sus modelos de negocio, entregando asesoría técnica, estratégica, seguridad, experiencia, análisis de modelos financieros y de negocio, desarrollos y prototipos. Las empresas asesoras apoyan a sus clientes durante toda la etapa de los proyectos, desde la idea inicial hasta el posicionamiento del producto final en los nuevos mercado. Las principales empresas de asesoramiento en tecnología blockchain son:

- **Blockchain App Factory:** entrega asesoramiento sobre la implementación estratégica de la tecnología blockchain. Proporciona orientación, capacitación y enseña a través de seminarios, talleres sobre la tecnología blockchain y la aplicación relevante.
- **DigitalX:** Ofrece una amplia gama de servicios de consultoría de seguridad y desarrollo, desde servicios de diligencia y pruebas de seguridad hasta análisis de modelos de negocios y desarrollo de software.
- **MLG Blockchain:** Proporciona consultoría de desarrollo de blockchain, servicios de marketing y aumento de capital. Apoyados por sus asociaciones empresariales que llevan a la inclusión en los principales intercambios internacionales.

La propuesta de valor de estas organizaciones se basa en el desarrollo de estrategias y modelos de negocio en base a la experiencia, conocimiento y asociaciones que poseen dentro del ecosistema blockchain.

10.2. Modelo Ecosistema Blockchain

De acuerdo con el análisis realizado a cada uno de los actores del ecosistema Blockchain, considerando sus propuestas de valor, clientes, infraestructura y viabilidad financiera, se logra entender cuáles son las relaciones que poseen y como se agrega valor a lo largo de la cadena de la industria.

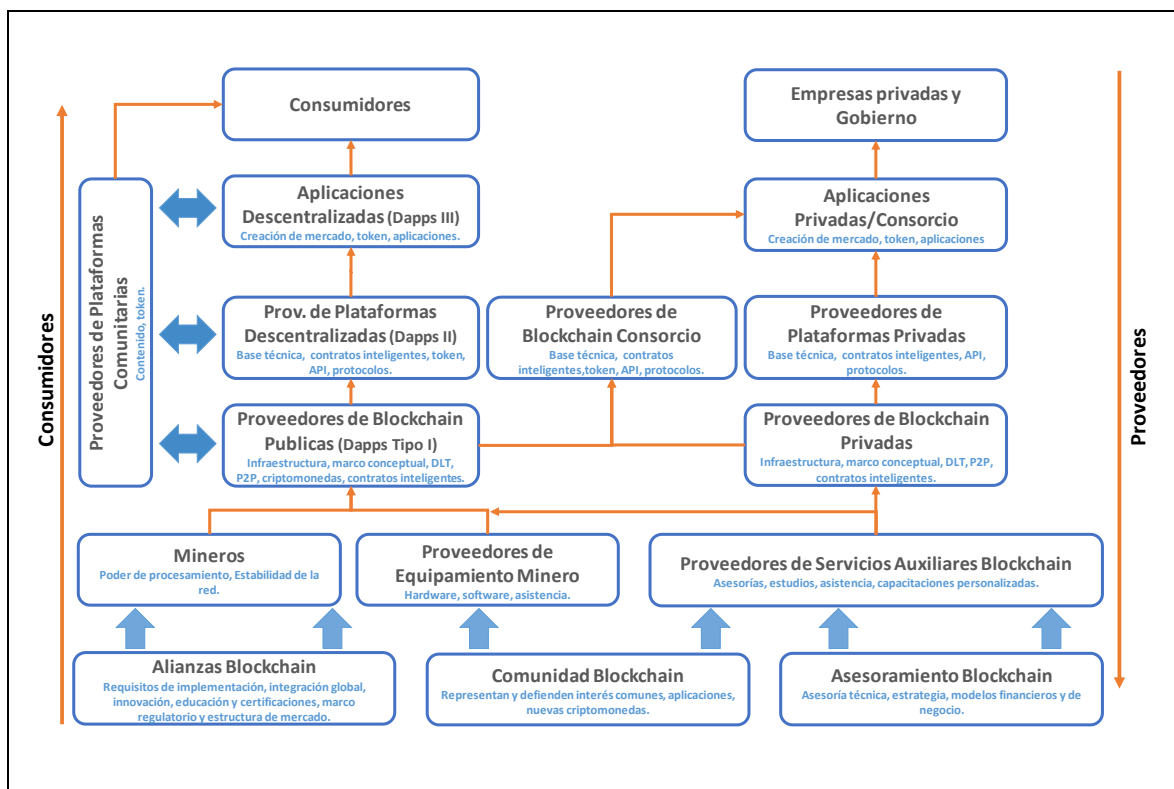


Ilustración N°4. Modelo Ecosistema Blockchain.

El modelo propuesto en la Ilustración N°4, permite entender el ecosistema blockchain. En la base del modelo se encuentran las alianzas, comunidades, y

servicios de asesoría, quienes son los encargados de potenciar el ecosistema mediante el establecimiento de requisitos de implementación, educación y asesoría en términos técnicos y estratégicos, marco regulatorio y estructura de mercado. Son actores consolidados dentro de la industria debido a su experiencia y a las alianzas obtenidas con importantes industrias interesadas en el desarrollo de la tecnología y su futura utilización.

En un segundo nivel se encuentra la industria de la minería representada por los mineros y proveedores de equipos y software minero, siendo una industria altamente competitiva de acuerdo a la cantidad de mining pool existentes para las principales blockchain públicas, presenta altas barreras de entrada en cuanto al uso intensivo de activos fijos para obtener el poder de cómputo necesario, para mantener la estabilidad de la red y obtener beneficios para el negocio. Por lo tanto la mejor forma de ingresar al negocio de la minería es unirse a uno de estos grupos mineros y obtener beneficios de acuerdo a la contribución realizada, sin embargo no se garantiza rentabilidades positivas debido a que la estrategia de recompensas de las pruebas de trabajo (POW), es que cada cierta cantidad de criptomonedas entregadas como recompensa aumenta la dificultad de la prueba y disminuye la cantidad recompensada. De esta manera se requiere mayor capacidad de cómputo y consumo energético para una menor cantidad de criptomonedas como recompensa. En cuanto a los proveedores de servicios auxiliares buscan el desarrollo del ecosistema mediante asesorías, asistencia técnica y estratégica, con equipos humanos altamente capacitados y experimentados, por lo que generan altas barreras de entrada a nuevos competidores al poseer una alta capacidad intelectual.

El tercer nivel está compuesto por los proveedores de infraestructura, blockchain públicas, consorcio y privadas, son las encargadas del desarrollo de la tecnología y su marco conceptual, requieren alto nivel de I&D y desarrolladores altamente competitivos. El sector está dominado por Bitcoin

(2009), Ethereum (2014), Ripple (2012), Hiperledger (2015), R3 (2014), organizaciones con experiencia y un gran desarrollo de la tecnología, las plataformas esta creadas sobre sus propias blockchain, permitiendo una mayor interoperabilidad y seguridad. Por lo tanto es difícil el ingreso de competidores o nuevos participantes en este nivel del ecosistema, además los proveedores de infraestructura están respaldados por una gran cantidad de importantes inversores y reconocidas empresas líderes en sus industrias.

En el cuarto nivel se encuentran los proveedores de plataforma, son los encargados de entregar los protocolos, API, bases técnicas, contratos inteligentes ajustados según requerimientos y token. Este nivel no existe concentración ya que posee una gran cantidad de participantes que compiten por entregar herramientas amigables y de fácil uso para la creación de aplicaciones. Si bien es un nivel de gran requerimiento de capacidad intelectual y experiencia no supone una gran barrera de entrada para nuevos competidores.

En el quinto nivel se encuentran los proveedores de aplicaciones descentralizadas (DApps tipo III), consorcio y privadas, son quienes crean el mercado entregando soluciones al usuario final que se puede encontrar en la mayorías de las industrias. En este sector del ecosistema es donde se refleja lo disruptivo de la tecnología blockchain y se presentan las mayores oportunidades de generar impactos, mientras la generación de aplicaciones descentralizadas permite modificar los modelos de negocios actuales, generando beneficios para la comunidad, aportando al desarrollo económico, disminuyendo la desigualdad y reduciendo costos al sacar a un tercero del medio, las aplicaciones privadas y de consorcio permiten mejorar los procesos de transacciones existentes principalmente en la industria financiera y cadena de suministro.

Las oportunidades de negocio en este nivel están asociadas a las DApps y pueden ser monetizadas al cobrar bajas tarifas por usos, se debe considerar que al tener códigos abiertos pueden ser replicadas y puestas en marchas con el cobro de una tarifa menor e incluso sin costo, pensando en que la idea de la descentralización es el beneficio de la comunidad. Sin embargo apostar a la adquisición de tokens en una ICO puede generar grandes dividendos si el proyecto en cuestión logra un éxito en el mercado, es este caso dependerá de la capacidad del inversor para detectar buenas opciones y la oportunidad de ingresar en una fase temprana para obtener mejores beneficios. La facilidad para entrar es este mercado dependen de la solución requerida y de la industria a la que pertenece el problema.

El sexto nivel del ecosistema corresponde a los consumidores finales, personas, empresas privadas y gobiernos, quienes juegan un papel fundamental al indicar sus requerimientos de solución a un problema específico, generando así un mercado o participando de la comunidad y alianzas blockchain para el desarrollo de la tecnología y el ecosistema.

Además existen los proveedores de plataformas comunitarias que requieren los servicios de proveedores de infraestructura, plataformas y aplicaciones para la construcción de sus sitios, donde se genera contenido para usuarios comunes o contenido técnico relacionado a blockchain que sirve para quienes son sus proveedores. Este es otro nivel del ecosistema donde se pueden generar grandes impactos al competir con modelos de negocio existentes como redes sociales y de contenido, donde los beneficiados son quienes crean comunidades y publican contenido.

El modelo propuesto es importante para entender la tecnología blockchain como un ecosistema, ya que su potencial está en la adopción y crecimiento de la red para el beneficio de toda la comunidad. Con él se puede comprender los

alcances comerciales de la tecnología, su impacto y generación de nuevas oportunidades de negocio. Además sirve como guía para posteriores investigaciones, ya que permite ubicarse en el entorno y entender la importancia de cada uno de los participantes del ecosistema.

Conclusiones

Actualmente la tecnología blockchain se encuentra en etapa de crecimiento apoyado por grandes empresas que apuestan por su desarrollo y potenciales usos. Existen una variedad de industrias en el ámbito privado que ven a la tecnología blockchain como una forma de mejorar sus procesos reduciendo tiempos de procesos, reducción de costos, aumento de la seguridad, transparencia y estabilidad del sistema. Sin embargo el verdadero potencial de la tecnología se puede apreciar en una red mayor mediante una rápida adopción, con la generación de nuevos modelos de negocio mediante aplicaciones públicas descentralizadas apoyando el desarrollo de la infraestructura en un aspecto económico, empresarial y social. Sin embargo, la adopción requiere de la articulación tanto del ámbito tecnológico como político, social y económico para llegar a una fase de maduración, si hoy existe un ecosistema robusto aun falta el desarrollo en temas relacionados a la regulación y al conocimiento por parte del macroentorno.

El análisis de la tecnología blockchain requiere de la comprensión total de su ecosistema, entendiendo el aporte generado a través de la cadena de valor de la industria por cada uno de los actores de acuerdo a sus modelos de negocios. Esto permite evaluar posibilidades de generación de nuevos modelos de negocios, reestructuración de los existentes para las empresas que serán impactadas y la creación de nuevos negocios que utilicen el desarrollo actual de la tecnología.

Si bien en la actualidad la tecnología blockchain está siendo adoptada principalmente por la industria financiera, para la mejora de sus procesos y sus servicios, también es factible su utilización en otros sectores del ámbito privado como cadena de suministro, legal, salud, social, educación, energía y sustentabilidad. Sin embargo son las empresas que basan sus modelos de

negocio en el registro e intercambio de información y valor mediante cualquier clase de activos las que poseen un mayor riesgo de ser impactadas económica y financieramente por la tecnología blockchain, por medio de las aplicaciones descentralizadas que buscan el beneficio de todos sus miembros. Este tipo de empresas deben buscar formas de reducir las amenazas de la tecnología ya sea incorporándola o ajustando sus modelos de negocio.

El objetivo general de la tesina es conocer el entorno de negocios de la tecnología blockchain, así como sus usos, repercusiones y beneficios para los negocios. Como el entorno de blockchain posee una gran cantidad de actores relevantes, el análisis mediante al ecosistema propuesto y la descripción de los modelos de negocios de sus participantes permiten entender cómo se agrega, entrega y captura valor a través de la cadena de valor de la industria creando modelos negocio o modificando los existentes. De esta manera, tenemos que el sector privado actualmente adopta la tecnología blockchain de tipo privada y consorcio para la mejora de sus procesos beneficiando su captura de valor, mientras la blockchain pública es utilizada mediante aplicaciones descentralizadas para construir modelos de negocios confiables, transparentes que distribuyen sus beneficios con la comunidad agregando y entregando valor.

Se espera que la investigación y sus resultados contribuyan a futuros estudios como punto de partida sobre la tecnología blockchain, sus beneficios para las distintas industrias y adaptabilidad de sus modelos de negocio. Líneas investigativas que podrían surgir a partir de este trabajo son el análisis del macroentorno de la tecnología blockchain, marco regulatorio y estado del ecosistema en Chile.

11. Bibliografía

- Abeyratne, S. A., & Monfared, R. P. (2016). Blockchain Ready Manufacturing Supply Chain Using Distributed Ledger. *International Journal of Research in Engineering and Technology*, 5, 1-10.
- Bermúdez, A. M. (2016). *Estudio de la utilización de protocolos blockchain en sistemas de votación electrónica*. Barcelona.
- Caballero, J. (2018). *Estudio de tecnologías Bitcoin y Blockchain*. Tesis, Universidad Oberta de Catalunya.
- Carson, B., Romanelli, G., Walsh, P., & Zhumaev, A. (Junio de 2018). *Mckinsey&Company*. Obtenido de <https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value>
- Chen, & Yan. (2018). Blockchain tokens and the potential democratization of entrepreneurship and innovation. *Business Horizons*, Volume 61, Issue 4, 567-575.
- Chen, Y. (2018). Blockchain tokens and the potential democratization of entrepreneurship and innovation. *Business Horizons*, Volume 61, Issue 4, 567-575.
- Chesbrough, H. (2010). Business Model Innovation: Opportunities and Barriers. *Long Range Planning*, 43, 354-363.
- Efanov, D., & Roschin, P. (2018). The All-Pervasiveness of the Blockchain Technology. *Procedia Computer Science*, 123, 116-121.
- Ethereum*. (2018). Obtenido de <https://miethereum.com/smart-contracts/dapps/#toc16>
- Forbes, I. (Noviembre de 2016). *Forbes Insights*. Obtenido de https://www.forbes.com/forbesinsights/sap_transactions/index.html
- Gimeno, J. C. (2018). *Estudio de tecnologías Bitcoin y Blockchain*. Obtenido de <http://hdl.handle.net/10609/81268>
- Gönenç Gürkaynak, I. Y. (2018). Intellectual property law and practice in the blockchain realm. *Computer Law & Security Review*, 34, 847-862.

- Gordon, W. J., & Catalini, C. (2018). Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability. *Computational and Estructural Biotechnology Journal*, 16, 224-230.
- Huckle, S., Bhattacharya, R., White, M., & Beloff, N. (2016). Internet of thing; Blockchain and Share Economy Applications. *Procedia Computer Science*, 98, 461-466.
- Hwang, J., Choi, M.-i., Lee, T., Jeon, S., Kim, S., Park, S., & Park, S. (Diciembre de 2017). Energy Prosumer Business Model Using Blockchain System to Ensure Transparency and Safety. *Energy Procedia*, 141, 194-198.
- Kshetri, N. (2018). Blockchain's roles in meeting key supply chain management objectives. *International Journal of Information Management*, 39, 80-89.
- Lérida, J. L., & Pérez, J. J. (2016). *La economía de Blockchain - Los modelos de negocio de la nueva web*. Creative Commons.
- Macías, M. (11 de marzo de 2012). *Advenio Strategy&Business and Design*. Obtenido de <http://advenio.es/crea-tu-business-model-canvas-con-google-docs/>
- Melanie Swan. (2018). Blockchain for Business: Next-Generation Enterprise Artificial Intelligence Systems. *Advances in Computers*, 11, 121-162.
- Meunier, S. (2018). Blockchain 101: What is Blockchain and How Does This Revolutionary Technology Work? *Transforming Climate Finance and Green Investment with Blockchains.*, 23-34.
- miethereum. (29 de Agosto de 2014). Obtenido de <https://miethereum.com/mineria/>
- miethereum. (2018). *Ethereum*. Obtenido de <https://miethereum.com/smart-contracts/dapps/#toc1>
- Millard, C. (2018). Blockchain and law: Incompatible codes? *Computer Law & Security Review*, 34, 843-846.
- Najmaei, A. (2015). Business Model Value Creation, Value Capture, and Information Technologies. *Encyclopedia of Information Science and Technology, Third Edition*, 549-557.

- Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Obtenido de <https://bitcoin.org/es/>
- Nasdaq. (2016). *Business Nasdaq*. Obtenido de https://business.nasdaq.com/Docs/Blockchain%20Report%20March%202016_tcm5044-26461.pdf
- Oh, J., & Shong, I. (2017). A case study on business model innovations using Blockchain: focusing on financial institutions. *Asia Pacific Journal of Innovation and Entrepreneurship*, 11, 335-344.
- Osterwalder, A., & Pigneur, Y. (2010). *Business Model Generation*. New Jersey: John Wiley & Sons, Inc.
- Porxas, N., & Conejero, M. (2018). Tecnología blockchain: funcionamiento, aplicaciones y retos jurídicos relacionados. *Actualidad Jurídica Uriá Menéndez*, 48, 24-36.
- Preukschat, A. (2017). *Blockchain la revolución industrial de internet*. Paidós Empresas.
- Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. *Future Generation Computer Systems*, 88, 173-190.
- Riasanow, T., Burckhardt, F., Setzke, D. S., Böhm, M., & Krčmar, H. (2018). The Generic Blockchain Ecosystem and its Strategic Implications. *Twenty-fourth Americas Conference on Information Systems*, 1-10.
- Santiago, I. (2016). *La Revolución de la Tecnología de las Cadenas de Bloques y su Impacto*. Sevilla. Obtenido de <https://ssrn.com/abstract=2846816>
- Sanz, J. M. (2017). *Blockchain per l'educació*. Barcelona. Obtenido de <https://ddd.uab.cat/record/181567>
- Supranee, S., & Rotchanakitumnuai, S. (2017). The Acceptance of the Application of Blockchain Technology in the Supply Chain Process of the Thai Automotive Industry. *Proceedings of The 17th International Conference on Electronic Business*, 30, 252-257.
- Swan, M. (2015). *Blockchain Blueprint for a New Economy*. O'Reilly .

Teece, D. J., & Linden, G. (2017). Business models, value capture, and the digital enterprise. *Journal of Organization Design*, 1-14.

Viriyasitavat, W., & Hoonsopon, D. (2018). Blockchain characteristics and consensus in modern business processes. *Journal of Industrial Information Integration*.

Zhang, P., Schmidt, D. C., & Jules White, G. L. (2018). Blockchain Technology Use Cases in Healthcare. *Advances in Computers*, 111, 1-41.

Zhao, J. L., Fan, S., & Yan, J. (2016). Overview of business innovations and research opportunities in blockchain and introduction to the special issue. *Financial Innovation*, 2, 1-7.