UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE QUITO

CARRERA DE INGENIERÍA DE SISTEMAS

ESTADO DEL ARTE ACTUAL CON RESPECTO AL BLOCKCHAIN EN RELACIÓN CON SU CONCEPTO, ELEMENTOS, FUNCIONAMIENTO Y APLICACIONES UTILIZANDO LA METODOLOGÍA SLR Y SYSTEMATIC MAPPING

Trabajo de titulación previo a la obtención del

Título de Ingeniero de Sistemas

AUTOR: Jhon Sebastián Andrango Quishpi

TUTOR: Gustavo Ernesto Navas Ruilova

Quito – Ecuador

2022

CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

Yo, Jhon Sebastián Andrango Quishpi, con documento de identificación N° 1726466756, manifiesto que:

Soy el autor y responsable del presente trabajo; y, autorizo a que sin fines de lucro la Universidad Politécnica Salesiana pueda usar, difundir, reproducir o publicar de manera total o parcial el presente trabajo de titulación.

Quito, 2 de marzo del año 2022

Atentamente,

Jhon Sebastián Andrango Quishpi
1726466756

CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE TITULACIÓN A LA UNIVERSIDAD POLITÉCNICA SALESIANA

Yo, Jhon Sebastián Andrango Quishpi, con documento de identificación N° 1726466756, expreso mi voluntad y por medio del presente documento cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autor del artículo académico: "Estado del arte actual con respecto al Blockchain en relación con su concepto, elementos, funcionamiento y aplicaciones utilizando la metodología SLR y Systematic Mapping", el cual ha sido desarrollado para optar por el título de: Ingeniero De Sistemas, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En concordancia con lo manifestado, suscribo este documento en el momento que hago la entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.

Quito, 2 de marzo del año 2022

Atentamente,

Jhon Sebastián Andrango Quishpi

1726466756

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Gustavo Ernesto Navas Ruilova con documento de identificación N° 1705675625, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: "ESTADO DEL ARTE ACTUAL CON RESPECTO AL BLOCKCHAIN EN RELACIÓN CON SU CONCEPTO, ELEMENTOS, FUNCIONAMIENTO Y APLICACIONES UTILIZANDO LA METODOLOGÍA SLR Y SYSTEMATIC MAPPING", realizado por Jhon Sebastián Andrango Quishpi con documento de identificación N° 1726466756, obteniendo como resultado el trabajo de titulación bajo la opción de Articulo Académico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Quito, 2 de marzo del año 2022

Atentamente,

Ing. Gustavo Ernesto Navas Ruilova, MSc.

1705675625

ESTADO DEL ARTE ACTUAL CON RESPECTO AL BLOCKCHAIN EN RELACIÓN CON SU CONCEPTO, ELEMENTOS, FUNCIONAMIENTO Y APLICACIONES UTILIZANDO LA METODOLOGÍA SLR Y SYSTEMATIC MAPPING

CURRENT STATE OF THE ART REGARDING THE BLOCKCHAIN IN RELATION TO ITS CONCEPT, ELEMENTS, OPERATION AND APPLICATIONS USING THE SLR AND SYSTEMATIC MAPPING METHODOLOGY

Andrango Quishpi Jhon Sebastián[1], Navas Ruilova Gustavo Ernesto[2]

Resumen

Blockchain es una tecnología que ha sido reconocida por el buen manejo de los datos y, sobre todo, la fornida seguridad que mantiene en su cadena de bloques es por ello que se conoce de manera más detallada en el presente artículo como llega a ese objetivo mediante la combinación de varios elementos. Todo esto se llevó a cabo mediante la recolección de información a través de un caso de estudio basado en la metodología de Systematic Mapping Study. En consecuencia, se encontró información relevante con respecto a la definición actual acerca de Blockchain, teniendo en cuenta los diferentes elementos que componen la cadena de bloques y su funcionamiento respectivo, dando como resultado, aplicativos basados en la arquitectura de esta tecnología. A esto se le añade un análisis FODA mediante el cual se presenta un enfoque más crítico con respecto a Blockchain, determinando la viabilidad de su implementación, en donde, el usuario conoce un punto de vista diferente, conociendo las implicaciones que conlleva su ejecución.

Palabras Clave: Blockchain, Funcionamiento, Aplicaciones, Elementos.

Abstract

Blockchain is a technology that has been recognized for its good data management and, above all, the strong security it maintains in its blockchain, which is why this article provides a more detailed understanding of how it achieves this objective through the combination of several elements. All this was carried out by collecting information through a case study based on the Systematic Mapping Study methodology. Consequently, relevant information was found regarding the current definition of Blockchain, taking into account the different elements that make up the blockchain and its respective operation, resulting in applications based on the architecture of this technology. To this is added a SWOT analysis through which a more critical approach to Blockchain is presented, determining the feasibility of its implementation, where the user knows a different point of view, knowing the implications of its execution.

Key Words: Blockchain, Operation, Applications, Elements.

[1] Estudiante de Ingeniería de Sistemas – UPS - Sede Quito. Autor para correspondencia: jandrangoq@est.ups.edu.ec

[2] Máster Universitario en Ciencias y Tecnologías de la Computación. Docente de la carrera de Ingeniería de Sistemas – UPS - Sede Quito. Email: gnavas@ups.edu.ec

1. INTRODUCCIÓN

Blockchain con el pasar del tiempo ha tenido un crecimiento bastante considerable debido a la efectividad que proporciona su funcionamiento en varios aspectos en los cuales se lo ha implementado, teniendo en cuenta siempre que las transacciones sean transparentes para los usuarios. En consecuencia, "las tecnologías de la computación han presentado una evolución yendo desde un modo centralizado hasta un modo descentralizado en lo referente a almacenamiento, poder de cómputo, infraestructura, protocolos y código" [1].

Por lo tanto, se presenta información con la cual se conoce las diferentes ventajas que tiene esta tecnología en cuanto a su combinación con las criptomonedas en donde Blockchain aparece como "una solución descentralizada sin ninguna organización de terceros en el medio. Cada transacción es validada por consenso de los participantes" [2].

De esta manera se analiza información más reciente sobre Blockchain teniendo en cuenta que su aplicación puede ser incluida más allá de las criptomonedas, sino más bien puede ser utilizada en diferentes ámbitos que hasta la actualidad se creía que no era posible su combinación.

Sin embargo, debido a que Blockchain utiliza métodos de consenso entre los diferentes nodos que contiene la red, esto provoca que "la red de la cadena de bloques no necesita ser confiable y puede intercambiar datos basados en direcciones en lugar de identidades personales" [2] dando como resultado negativo la influencia de varios usuarios para la aprobación de cualquier movimiento, lo cual puede traer consigo consecuencias bastante críticas, debido a la existencia de personas con ideales dañinos para la red, los cuales son capaces de tener un poder transaccional fuerte en la Blockchain, causando que se corrompa las transacciones en la red.

Esto ha provocado que se desconozca en su gran mayoría las verdaderas ventajas que tiene, provocando el temor de los usuarios al momento de enterarse que cualquier aplicativo que están usando, en su interior tiene una arquitectura basada en la tecnología Blockchain.

En el presente artículo se presenta un enfoque diferente con respecto a la temática principal de Blockchain ya que se analiza el impacto de esta tecnología viéndolo desde el punto de vista de su implementación en el Bitcoin y la relación que lleva con las demás criptomonedas que existen en la actualidad, en donde, se obtiene una concepción acerca de blockchain, que en términos simples se la pude describir como "una base de datos en la que cualquiera puede almacenar información, entre ellas las transacciones de criptomonedas" [3].

Posteriormente, se presentan los elementos que hacen posible que pueda desarrollarse correctamente, teniendo en cuenta siempre a seguridad que implementa Blockchain con la finalidad de garantizar que los datos se mantengan siempre privados, dando como consecuencia que los datos no puedan ser interpretados por ningún motivo, a pesar de ser divulgados por algún usuario mal intencionado.

Además, se presenta los diferentes aplicativos que existen actualmente que tienen en su interior a la cadena de bloques como parte fundamental para su funcionamiento puesto que "Blockchain como conector de software ayuda a hacer consideraciones de arquitectura explícitamente importantes sobre el rendimiento resultante y los atributos de calidad del sistema" [4] lo cual contribuye a que se optimice de mejor manera el uso de los recursos dando como resultado que las transacciones culminen exitosamente entre dos usuarios. Por lo tanto, se va a contribuir con información reciente con respecto a Blockchain, abordado puntos específicos de ésta, con el objetivo de presentar datos relevantes que ayuden a comprender el impacto que puede tener la cadena de bloques en los usuarios, cuando se está considerando como idea principal su combinación con algún aplicativo en desarrollo.

2. METODOLOGÍA

En este artículo, con el objetivo de seleccionar la mejor metodología para la elaboración del presente escrito, se pone en contexto dos metodologías, las cuales actualmente son utilizadas para la recolección de información de gran calidad por parte de trabajos técnicos que han sido publicados en diferentes bibliotecas virtuales, para lo cual es necesario conocer cada una de ellas con la finalidad de seleccionar una de ellas para la ejecución del estado del arte respectivo con respecto a la temática principal, siendo ésta Blockchain.

2.1. Systematic Literature Review (SLR)

Cuando se habla de SLR, por sus siglas en inglés Systematic Literature Review, en términos generales se la puede definir como una metodología la cual es utilizada para la recolección de información de gran calidad de manera sistemática , en donde, se realiza una revisión literaria con el objetivo de recopilar lo más importante de trabajos investigativos para posteriormente realizar un análisis de carácter de los datos relevantes que fueron seleccionados con el fin de llegar a una especie de resumen definido con la cual se puede satisfacer las preguntas de investigación que intervienen en el proceso. A continuación, se muestran los pasos que intervienen en la metodología:

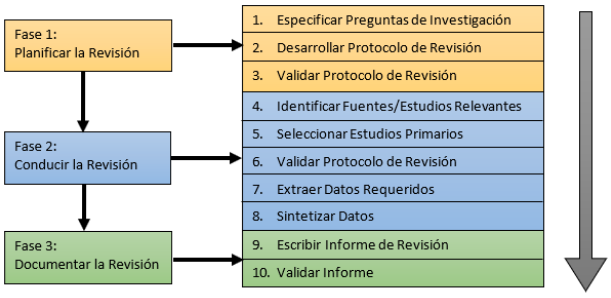

Figura *1*. Proceso de Systematic Literature Review (traducido al español del original)

Como se puede observar en la Figura 1 [5], se muestra como la metodología SLR realiza la selección de los datos basándose en un proceso de 10 pasos, en donde el punto de partida para la recopilación de información es la especificación de las respectivas preguntas de investigación con las cuales se busca satisfacer las necesidades que el investigador requiere para su trabajo investigativo, terminando con la escritura y validación de la información que se encuentra impresa en un informe o resumen como se mencionó anteriormente.

Es importante tener en cuenta que cada paso que se involucra en este proceso es relevante para el desarrollo adecuado de la metodología, ya que la exclusión o evasión de alguno de estos puede tener consecuencias al momento de obtener los resultados finales en cuanto a los datos recolectados de las diferentes fuentes que fueron consultadas por parte del usuario que lo implementa en su investigación.

2.2. Systematic Mapping Study (SMS)

Por otro lado, aparece SMS como la segunda metodología a tener en cuenta para el desarrollo del presente artículo que, como es de conocimiento general, se caracteriza por realizar un mapeo sistemático a la información que se va obteniendo a partir del título y el resumen del trabajo científico seleccionado. En otras palabras, se puede resumir que la implementación de este proceso se debido a que “están diseñados para brindar una descripción general de un área de investigación a través de la clasificación y el conteo de contribuciones en relación con las categorías de esa clasificación” [6].

Teniendo en cuenta estas particularidades con respecto a este procedimiento, al igual que la metodología anterior, SMS contiene una serie de 5 pasos que se enumeran a continuación, los cuales fueron propuestos por el autor Petersen con la finalidad de entregar de una manera simplificada el proceso que esta sigue para obtener un mapeo sistemático de la información.

1. Definición de preguntas de investigación (alcance de la investigación).
2. Realizar búsqueda de estudios primarios.

3. Selección de artículos para inclusión y exclusión.
4. Clasificación de los artículos.
5. Extracción y agregación de datos [7].

Como se puede evidenciar el primer paso para la recolección de datos es la creación de las preguntas de investigación las cuales son el hincapié al momento de seleccionar artículos para posteriormente seguir con las siguientes etapas de recolección de datos, dando como resultado la extracción de una información de carácter sistemático, la cual ha seleccionado los datos más representativos en base a la investigación que se desea realizar.

Al conocer ambas metodologías es posible distinguir ciertas similitudes entre la una y la otra ya que en sus pasos implementan ciertos puntos en común, pero a la vez, tiene una diferencia al momento de tratar la información en sus diferentes etapas, y, es asi que se considera que son diferentes al momento de plantear los objetivos que se buscan satisfacer, lo cual provoca que el enfoque al momento de analizar los datos sea diferente. De esta manera, "mientras que las revisiones sistemáticas tienen como objetivo sintetizar la evidencia, considerando también la fuerza de la evidencia, los mapeos sistemáticos se preocupan principalmente por estructurar un área de investigación" [6].

Al conocer la diferencia entre ambas metodologías se opta por aplicar en el presente Estado del Arte la metodología de Systematic Mapping Study (SMS) debido a que, con su facilidad de recolectar información a través de su título, palabras claves y resumen, facilita la exclusión de trabajos que no tienen coincidencia o información relevante con la temática principal del escrito a ser realizado optimizando el tiempo de búsqueda y selección de artículos en las diferentes bibliotecas virtuales.

3. CASO DE ESTUDIO SOBRE BLOCKCHAIN CON SYSTEMATIC MAPPING STUDY

Por lo tanto, se empieza el desarrollo de este proceso de SMS con la declaración de las preguntas de investigación o mejor conocidas como Research Question, las cuales serán las encargadas de encaminar la investigación hacia los principales puntos con respecto a la temática de Blockchain y, a su vez, especificar el alcance que va a tener la investigación.

3.1. Research Question

1. ¿Cuáles el estado actual del Blockchain?
2. ¿Qué tópicos se tratan sobre Blockchain?
3. ¿Qué elementos forman parte del proceso de Blockchain y cuál es su funcionamiento?
4. ¿Qué aplicaciones se han desarrollado en base a la tecnología de Blockchain en los diferentes ámbitos que existen?

Después de realizar las preguntas respectivamente se procede a estructurar una cadena de búsqueda con la cual se espera satisfacer los puntos expuestos en las preguntas de investigación para la recolección de trabajos científicos con información para el escrito.

"Blockchain" OR "blockchain types" OR "what is it blockchain" OR "how it works blockchain" OR "blockchain elements" OR "blockchain applications" OR "Blockchain protocols"

Al ejecutar esta cadena de búsqueda se obtiene un grupo reducido de artículos en los cuales se puede observar que empieza a reducir la cantidad de datos. Estos datos se reflejan en la tabla a continuación.

Tabla *1*. Numero de artículos por cada biblioteca virtual

Bibliotecas Virtuales	Número de Artículos
IEEE	10
ACM – Digital Library	15
ScienceDirect	7
ResearchGate	14
Google Scholar	18
Total	**64**

Como se puede observar, al momento de realizar la búsqueda con la cadena mencionada anteriormente se obtuvo 64 artículos para ser analizados, con los cuales, el siguiente paso para el análisis de los datos es el establecimiento de criterios de inclusión y exclusión, los cuales se presentan a continuación en la Tabla 2.

3.2. Criterios de inclusión y Exclusión

Tabla *2*. Criterios de Inclusión y Exclusión

Inclusión	Exclusión
Artículos y tesis en los cuales se pueda apreciar la inclusión de la temática de Blockchain como tal. (I1)	Libros, artículos y tesis que no contengan información importante o necesaria para la investigación. (E1)
Búsqueda de información en bibliotecas digitales con gran cantidad de artículos enfocados a la rama de la ingeniería de sistemas. (I2)	Información que no sea relevante en cuanto al área en la que se aplica. (E2)
Tener en cuenta el título, resumen y palabras claves que contengan información relacionada al tema de Blockchain. (I3)	Toda la información que no contenga la temática Blockchain. (E3)
Información relevante en cuanto a los puntos importantes de Blockchain a tratarse en un rango de tiempo no menor al año 2015. (I4)	Toda la información que sea menor al año mencionado en cuestión. (E4)

De acuerdo con la información que se menciona anteriormente, se procede a la selección con más cautela de los artículos que fueron seleccionados en un principio, teniendo en cuenta como parámetro de filtro los criterios de inclusión y exclusión, los cuales van a ser de utilidad para la recolección adecuada de los datos en base al objetivo que se tiene planteado por parte del tema a ser desarrollado en la investigación. Por lo tanto, al aplicar este proceso se obtiene una nueva cantidad de artículos los cuales se muestran en la Tabla 3.

Tabla *3*. Selección de Artículos Según Criterios de Inclusión y Exclusión

Criterios	Número de Artículos
I1	5
I2	3
I3	6
I4	11
Total Inclusión (T1)	**25**
E1	14
E2	10
E3	9
E4	6
Total Exclusión (T2)	**39**
Total (T1 +T2)	**64**

3.3. Screening of Papers

Al momento de realizar un análisis en base a los criterios de inclusión y exclusión expuestos en la Tabla 2, se puede observar que la reducción de los artículos en relación con la muestra inicial ha sido reducida en una cantidad considerable, dejando en evidencia la información más relevante que va a ser utilizada para el estudio

de Blockchain. Por lo tanto, se toma como referencia el valor expuesto en el apartado "T1" que se presenta en la Tabla 3, siendo éste el número de trabajos investigativos que contienen la mayor información con respecto a la temática principal del presente documento, y sus diferentes subdivisiones a desarrollarse, descartando un total de 39 artículos en los cuales no se aprecia información relevante que pueda servir de aporte para la elaboración del estado del arte.

3.4. Keywording

Como siguiente paso en el desarrollo de selección de información, se procede a establecer un conjunto de palabras clave (Keywording) en donde el objetivo de estas son las de mejorar la búsqueda de información dentro los trabajos investigativos, destacando lo más importante de cada documento y entregándole la debida importancia del caso. A continuación, se muestra la lista de palabras empleadas:

- Blockchain.
- Blockchain Types.
- Criptocurrency.
- Bitcoin.
- Blockchain Elements.
- Hard Fork.
- Protocols.
- Applications.
- Definition/Concepto
- Blockchain Technology
- Quorum
- Hyperledger
- Smart Contract
- Mineria/Minning
- Criptografia
- Consenso
- PoF
- PoW

Una vez definidas las mencionadas palabras claves se procede a la recopilación de la información, el cual es el último paso, ya que en este se realiza la extracción y mapeo de carácter sistemático a la información, la cual se obtiene realizando la lectura precisa en los puntos más relevantes de cada fuente de información seleccionada anteriormente por la metodología.

De esta manera, se puede concebir una definición con respecto al Keywording aplicado anteriormente, con el cual se puede indicar que la temática de Blockchain aparece en la mayoría de los artículos como una parte fundamental en sus implementaciones, así también, se conoce las diferentes partes que componen esta tecnología para que pueda ser eficaz en los ámbitos que se conocen actualmente.

3.5. Systematic Map

Finalmente, en esta última etapa de la metodología se procede a la presentación de las diferentes fuentes de información utilizadas para la recolección de los datos, teniendo en cuenta los diferentes filtros aplicados anteriormente, en donde, se obtiene como resultado final una muestra reducida de artículos, los cuales se presenta a continuación.

Tabla *4***.** Numero de Artículos por Biblioteca Virtual

Bibliotecas Virtuales	N.º de Artículos
ScienceDirect (L1)	4
ACM - Digital Library (L2)	6
ResearchGate (L3)	4
Google Scholar (L4)	7
IEEE Xplore (L5)	4
Total	**25**

En la Tabla 4, se puede apreciar que el total de los artículos seleccionados son de 25, en donde de L2 se han seleccionado 6 artículos mientras que de L4 se ha conseguido un total de 7, convirtiéndose en las bibliotecas que tienen mayor influencia en la investigación. Por lo tanto, librerías virtuales restantes L1, L3 y L5 se sabe que han aportado para el presente estado del arte con 4 artículos cada una, completando el valor total mencionado en un principio de

trabajos científicos. Para comprender de mejor manera el impacto de cada una se presenta a continuación un gráfico de pasteles con el porcentaje respectivo.

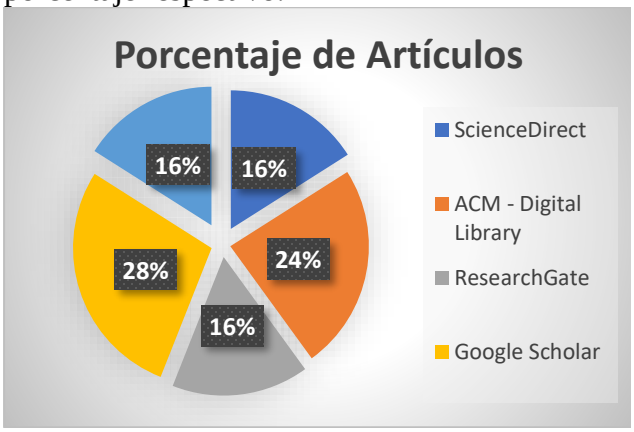

Figura *2*. Porcentaje de artículos por cada Biblioteca Virtual

La selección de los artículos se la realizo en base a la cantidad de información relevante que contienen estos, por esta razón se ha obtenido un numero especifico por cada repositorio consultado para obtener datos acerca de Blockchain, dando como resultado un total de 5 bibliotecas virtuales que fueron utilizadas como fuente de consulta. Por lo cual, se observa en la Figura 2 que Google Scholar y ACM – Digital Library son las librerías con mayor aporte para la investigación teniendo un 28% y 24% respectivamente.

Así también, de las demás fuentes de consulta mencionadas en la Ilustración 4, se obtuvo un 16% de cada una de ellas, aportando en menor cantidad con artículos académicos para el trabajo investigativo, pero manteniendo todas las etapas anteriormente propuestas por la metodología seleccionada para el desarrollo del documento.

Teniendo en cuenta esto, en base a los diferentes pasos que se aplican en la metodología, el primer resultado de la investigación es una serie de antecedentes los cuales son el pivote principal para tener un mejor entendimiento de Blockchain, los cuales se presentan a continuación:

3.6. Antecedentes de Blockchain en las Criptomonedas.

Para entender de mejor manera la tecnología Blockchain es necesario empezar por uno de los componentes que han dado a conocer a gran magnitud esta tecnología, la cuales son las criptomonedas, que, si bien se sabe, no es la única aplicación que tiene Blockchain en cuanto a los diferentes usos que se le ha dado, es por ello que se analiza en este ámbito para tener una referencia de como fue el punto de partida. Es asi que se empieza con las criptomonedas, desde su punto más básico hasta la implementación de Blockchain y su importancia en el desarrollo de cualquier criptodivisa que la utilice en su sistema interno de minería.

3.6.1. Creación de Criptomonedas

Para la creación como tal de este tipo de moneda digital hay que considerar dos aspectos que se los puede considerar como importantes ya que de esto depende el desarrollo de esta. En primer lugar, se considera si se la va a programar desde cero por uno mismo, siendo así, buscar un lenguaje de programación es esencial para la construcción de esta; al existir varios de estos, la mayoría de los autores sugieren como lenguajes principales para la creación de criptomonedas a C/C++ o Python.

Por otro lado, si la creación de esta criptodivisa se la quiere emplear de una manera más simplificada, en otras palabras, lejos de lo que se refiere a programación, en la actualidad han surgido aplicativos en los cuales se puede crear una de estas monedas con una interfaz gráfica ya sea mediante una página web o un programa ejecutable en el escritorio de una computadora.

De cualquier manera, cuando se produce la creación se mantiene presente que el procedimiento que realizan es similar en ambos casos con la diferencia que de una forma se puede ir construyendo paso a paso la moneda y se puede corregir ciertos errores que puedan aparecer en el proceso, mientras que de la otra forma solo se completa campos predeterminados que entrega la interfaz

considerados importantes para su respectiva configuración; con la particularidad que en ambos procesos existe un punto en común, siendo este, el uso de Blockchain.

Para la creación de una criptomoneda estos autores consideran cuatro elementos como necesarios para la construcción de esta.

- Identidades.
- Transacciones.
- Almacenamiento en Blockchain.
- Comunicación Peer to Peer [8].

Como se observa, Blockchain es una parte fundamental en el desarrollo de una criptomoneda puesto que para que una criptomoneda tenga un funcionamiento adecuado, es necesario que se distribuya por toda la red y se guarden los procedimientos que esta realiza en la web, por esta razón, "la solución que todas las criptomonedas de primera y segunda generación utilizan es la tecnología de blockchain o encadenamiento de bloques" [8].

Así también, además del método que se menciona anteriormente, existe otra forma de creación u obtención de criptomonedas, más conocido como minado de Criptomonedas, el cual se lo puede definir en términos generales como el proceso mediante el cual se puede producir divisas las cuales son conocidas actualmente por la mayoría de los autores como dinero digital.

3.6.2. Minería de Criptomonedas

Por otro lado, cuando se realiza una implementación de esta tecnología es importante conocer la minera de criptomonedas en la cual se procesan transacciones de una específica criptomoneda para realizar validaciones y sobre todo conseguir una transacción correcta de los valores. Como ejemplo en primera instancia se utiliza un Smart Contract: Ethereum que ha sido desarrollado para la criptomoneda denominada Ethereum en el cual se puede evidenciar la inclusión de Hard Fork para la mejora de su cadena de bloques y tener mayor control.

Es así, que en un principio se comprende como es el funcionamiento esta tecnología que indirectamente realiza un procedimiento de minería con la criptomoneda que éste utiliza. Por lo tanto, siendo más específico, el proceso de minería de Ethereum si se lo analiza de manera detallada se puede evidenciar que se parece en ciertos puntos al protocolo que implementa Bitcoin, por lo cual, al momento de realizar una minería como tal, los mineros son los encargados de escuchar las peticiones sobre las transacciones que se deben ejecutar en la Blockchain, dando como resultado, la adicción de dichas peticiones a un bloque de transacciones, en donde el sistema se encarga de comparar con los demás bloques con la finalidad de entregar como resultado un rompecabezas criptográfico. Es asi que una vez se obtenido esto, "si el minero resuelve el rompecabezas criptográfico primero, entonces el minero transmite el nuevo bloque a través de la red Ethereum y es recompensado con Ether recién acuñado" [9].

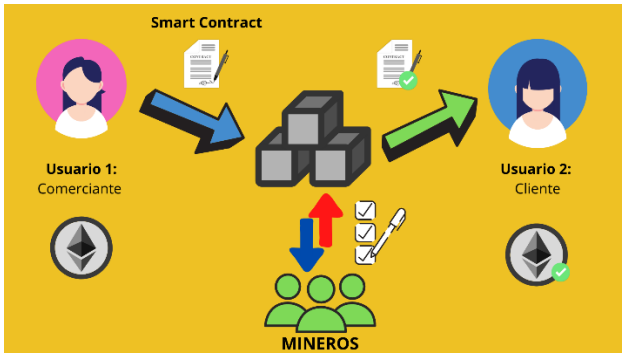

Figura 3. Funcionamiento de Smart Contract de Ethereum

Como se puede apreciar, en el procedimiento del Smart Contract con Ethereum los mineros son una parte fundamental para las transacciones de la criptomoneda que lleva el mismo nombre, agilitando de mejor manera el proceso de minería. Sin embargo, esta tecnología dio el inicio a otras formas de minería que se implementa con otro tipo de criptomoneda, por ejemplo, el bitcoin en el cual se ofrece un

procedimiento similar, pero utiliza una metodología denominada Bitmain que se encarga de realizar este proceso; por esta razón Ethereum sufre una evolución, por así decirlo, y refuerza su cadena de bloques mediante el uso de Hard Fork.

3.6.3. Hard Fork

Una bifurcación dura o Hard Fork, se produce cuando se implementa una nueva regla en la cadena de bloques antigua, dando como resultado un conjunto de bloques en los cuales la nueva normativa pasa a ser menos estricta y, en su defecto, lo convierte en un proceso inverso a lo que se conoce como Soft Fork. Por lo tanto, una definición de lo que es este procedimiento se lo puede resumir que Hard Fork sucede cuando una nueva norma o versión ha sido creada y se interna en la cadena de bloques, los nodos originales no aceptan este cambio debido a la existencia de los nodos nuevos que existen por lo cual una cadena de bloques que se tenía al principio pasa a ser dos cadenas que funcionan de manera simultánea.

Para entender de mejor manera como es el funcionamiento de esta tecnología, se pone en evidencia un ejemplo (Figura 4) propuesto por el autor Schär, en el cual se supone que algunas personas de la red Bitcoin desea aumentar el límite de tamaño de bloque de 1 MB a 2 MB y, por lo tanto, duplicar el número de transacciones que se pueden incluir en cada bloque. Cualquiera que esté aplicando la nueva regla puede producir bloques con un tamaño superior a 1 MB, es decir, mayor que el límite de las reglas de consenso originales. Cualquiera que esté aplicando el conjunto de reglas anterior rechazará estos bloques [10].

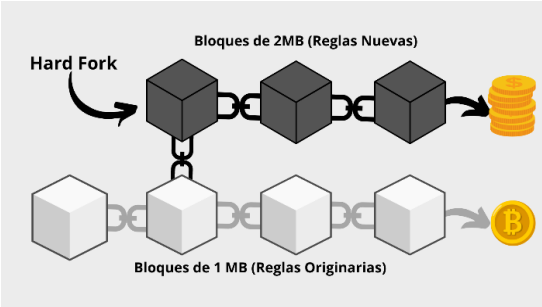

Figura *4*. Ejemplo de Hard Fork

3.6.4. Criptomonedas relevantes

Además del conocido Bitcoin, existen otras criptomonedas las cuales son actualmente importantes como el mencionado anteriormente. A continuación, se presenta un breve listado de algunas de las criptomonedas más conocidas actualmente que sobresalen y son utilizadas mundialmente.

- **Bitcoin:** Es una de las primeras implementaciones de un concepto denominado criptodivisa o criptomoneda, que consiste en una moneda virtual generada de forma descentralizada, por un único organismo, sin control de parte de algún gobierno y de un carácter anónimo. Esta moneda permite efectuar transacciones de forma segura y sin la necesidad de un intermediario financiero ni de pago de comisiones [11].
- **NEO:** Es una criptomoneda con la peculiaridad de que cada token de esta genera "tokens" de otro contrato llamado GAS, con el que se paga a los intermediarios de las transacciones con la misma, haciendo que en ninguna. transacción realizada con NEO suponga un pago con la misma a ningún intermediario [3].
- **Monero:** Es una criptomoneda segura, privada e imposible de rastrear que fue desarrollada en 2014 por un grupo de 7 desarrolladores, de los cuales 5 aún permanecen anónimos. Monero implementa, como el resto de las criptomonedas, una cadena de bloques (blockchain) para registrar las transacciones realizadas [12]. Como dato adicional, es importante conocer que, para mantener dichas normas de protección hacia los usuarios, basa su seguridad en un protocolo denominado CryptoNote.
- **Ripple:** Es la tercera criptomoneda más grande en la lista de monedas digitales líderes después de ethereum. Es una moneda controvertida debido al hecho de que esta moneda no está descentralizada, sino que es una criptomoneda centralizada que fue la

idea clave de blockchain. Aunque es la única criptomoneda centralizada, Ripple se puede utilizar para inversiones, ya que parece ser bueno [13].

- **Ethereum:** Ethereum es una versión modificada de bitcoin Satoshi Nakamoto. Fue fundada por Vitalik Buterin. Hace un par de años, Vitalik estaba trabajando con el diario de Bitcoin, estaba probando Bitcoin con un gran conocimiento de esa industria y allí imaginó o vio la oportunidad de extender la primera innovación de blockchain que fue bitcoin en éter [13].

4. BLOCKCHAIN

4.1. Definición

En términos generales, se considera a Blockchain como una tecnología que simula un libro contable en donde se almacenan las transacciones que realizan los usuarios sin necesidad que exista un intermediario de por medio para revisar o regular dicha transacción. Por otro lado, una concepción acertada a ésta es que "Blockchain es un libro mayor distribuido, inmutable, transparente, seguro y auditable, que registra todas las transacciones ejecutadas y las comparte entre todos los participantes" [2].

Por la versatilidad que esta tecnología tiene al momento de manejar las transacciones su aplicación en otros ámbitos la convierten en un proceso innovador para cualquiera que sea el uso del usuario; por esta razón, se la considera de gran utilidad para la implementación en algunos ámbitos específicos, en donde, Blockchain se encarga de abastecer un método con el cual se facilita la creación y ejecución de los conocidos Smart Contracts.

4.2. Tipos

Como es de conocimiento el desarrollo de Blockchain ha sido debido a su gran facilidad al momento de manejar datos de manera incógnita pero, a pesar de ser una tecnología de libre modificación, con la evolución a pasos agigantados de los diferentes procesos informáticos que existen actualmente, han traído como consecuencia la privatización de ciertas tecnologías por parte de las empresas de gran poder en el mundo e incluso, de gobiernos creando sistemas centralizados los cuales son administrados por una corporación en particular. Por lo tanto, Blockchain no es la excepción de este caso, por consiguiente, según la recopilación de varios autores que conocen acerca de esta temática, concuerdan que existen tres tipos de esta las cuales son publica, privada y federada o de consorcio.

4.2.1. Blockchain Privada

Cuando se habla de ser una conexión de carácter privado, también se puede tener en cuenta que la tecnología Blockchain tenga una estructura similar a la pública con la diferencia que se encuentra privatizada en cierto punto por un ente o autoridad que ha sido seleccionada. Por lo cual, siendo más específicos se puede decir que una Blockchain es privada cuando los nodos que intervienen en la operación requieren de una autenticación o un permiso de carácter único para el acceso a la red en la cual se desea trabajar, ya que sin esta credencial no va a ser posible observar la cadena de bloques, ni las transacciones que se realizan en el libro mayor. Es por ello, que el autor Mohan indica un contraste entre lo público y lo privado, el cual entrega como conclusión que "cuando se utiliza un sistema de cadena de bloques privado o con permiso, en una red Blockchain específica, solo las personas que están explícitamente autorizadas por los participantes o administradores actuales de esa red pueden formar parte de ella" [14].

Un ejemplo de Blockchain privada es la plataforma de Quorum la cual fue desarrollada por J.P Morgan para el uso en el ámbito financiero y económico, pero con el pasar del tiempo se le ha dado uso en otros apartados diferentes a los ya mencionados. Por ello, en esencia Quorum "es una Blockchain autorizada

basada en la cadena de bloques Ethereum. Más precisamente, es una bifurcación de go-ethereum" [15].

4.2.2. Blockchain Publica

En términos simples se puede definir este tipo de Blockchain como "una red a la que cualquier persona puede acceder puede crear bloques y puede participar en el proceso de consenso o proceso de validación" [16]. Sin embargo, la principal característica de este tipo de tecnología es que es totalmente descentralizada lo que significa que no existe control de ningún tipo de las operaciones que se realizan internamente en el aplicativo o, en su defecto, en las transacciones que se puede encontrar ejecutando en cualquier lugar del mundo por cualquier usuario, razón por la cual; la minería es una de las actividades más comunes en este tipo de tecnologías y, sobre todo, más conocidas cuando se habla del manejo criptomonedas.

Por otro lado, al hablar de un ejemplo en cuanto a este tipo se puede mencionar el ámbito de las criptodivisas y sus transacciones donde las más importantes que utilizan una Blockchain publica son Bitcoin y Ethereum; ya que estas mantienen el anonimato de sus usuarios y los procedimientos que estos realizan internamente debido a que, como se menciona anteriormente, la forma más utilizada en la obtención de una criptomoneda es mediante la minería, por lo cual el acceso es libre para cualquier persona natural que se inmiscuya en esto.

4.2.3. Blockchain Federada o de Consorcio

Al hablar de federada o de consorcio, se puede provocar cierto grado de confusión al momento de identificar este tipo de Blockchain, pero en términos simples se le puede decir que es un sistema el cual puede estar público en ciertos elementos, pero a su vez mantiene ciertas restricciones, las cuales pueden ser interpretadas como la parte privada que se le puede implementar a la cadena de bloques, siendo así que se le podría denominar un tipo hibrido o semiprivado de esta tecnología. Aunque es importante mencionar que en algunas ocasiones también se la ha considerado solo de carácter privativo, con el adicional que en este apartado puede controlar una organización en específico el manejo del Blockchain. La característica principal es que solo tiene un conjunto seleccionado de usuarios que son los encargados de controlar la cadena de bloques con la ventaja que puede funcionar en varias organizaciones que estén involucradas ya que "cada nodo del consorcio blockchain suele tener una entidad organizativa que le corresponde, pudiendo unirse y retirarse de la red previa autorización" [17]. Además, solo estos usuarios son los encargados de tener acceso al libro mayor de Blockchain ya que, a diferencia de los dos tipos mencionados anteriormente, no realizan procesos de bifurcación por lo cual evitan la intrusión de usuarios no autorizados al sistema sin autenticación previa. "La lectura puede ser pública o restringida a los participantes. Estas cadenas de bloques se pueden considerar «parcialmente descentralizadas»" [16].

Como se observa este tipo de Blockchain conlleva varias implicaciones para lograr su objetivo final, por lo cual un ejemplo de ello es la creación del grupo Hyperledger el cual es un apartado desarrollado para el crecimiento empresarial e industrial a través de procedimientos de Blockchain el cual fue construido bajo la tutela de Linux Foundation en colaboración con otras organizaciones que tuvieron una acogida positiva al marco de código abierto que mantiene la tecnología de cadena de bloques. De esta manera, se conoce que esta colaboración "se enfoca en marcos de blockchain con permiso en lugar de sin permiso para brindar el máximo apoyo a las empresas y organizaciones que desean utilizar la tecnología de blockchain para atender sus propias aplicaciones en el proceso de formación y desarrollo" [18].

4.3. Elementos y Funcionamiento

Para el funcionamiento adecuado de Blockchain en primera instancia es necesario conocer los

elementos que la componen, los cuales se detallan a continuación.

4.3.1. Bloques

En términos simples, un bloque es tan solo un conjunto de transacciones en donde, además de guardar los datos de la transacción a realizarse, se almacena información extra la cual sirve para su posterior almacenamiento en la cadena de bloques (Blockchain) después de su verificación y validación respectiva.

4.3.2. Nodos

Según el autor Navarro, se los conoce como computadoras conectadas a la red utilizando un software que almacena y distribuye una copia actualizada en tiempo real del Blockchain [19].

4.3.3. Mineros

Este elemento juega un papel fundamental en la cadena de bloques ya que es el encargado de verificar la validez de la transacción que se va a realizar para que a continuación consiga la autorización de ser añadido a la Blockchain respectivamente.

4.3.4. Métodos de Consenso

Son algoritmos desarrollados para mantener el control de los bloques que se añaden a la Blockchain, con la particularidad de que su funcionamiento se basa en un sistema de votación en el cual se relaciona la cantidad de elementos que un usuario puede controlar con el número de votos que éste tiene por parte de los demás miembros de la comunidad, dándole mayor credibilidad al momento de realizar revisiones a las transacciones o contratos que se pretenden ingresar al libro de cuentas. Actualmente los métodos que más se utilizan es el de Proof of the Work (PoW) y Proof of Stake (PoF). Sin embargo, existen varias derivaciones en base a estos algoritmos los cuales han sido adaptados según el caso de uso necesario.

4.3.5. Criptografía

De igual manera que los mineros, es importante este elemento para Blockchain ya que, en términos generales, su función es la de brindar seguridad a las transacciones que se realizan por las diferentes cadenas de bloques.

Una vez se conocen los elementos que conforman la tecnología Blockchain, se procede a explicar cómo intervienen éstos en el funcionamiento respectivamente. Para lo cual, en un principio se conocen de manera general los pasos que intervienen, los cuales se toma como referencia los propuestos por el autor Quesada que se muestran a continuación.

- Transacción.
- Bloques.
- Verificación.
- Hash.
- Ejecución de la Transacción [20].

Como se puede observar existen cinco pasos mediante los cuales se desarrolla esta tecnología de manera adecuada, por lo cual, a continuación, se desglosa estos pasos de manera más detallada.

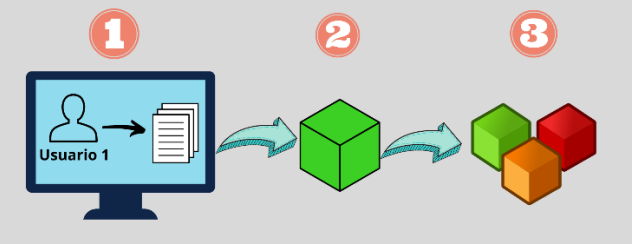

Figura 5**.** Funcionamiento Blockchain - Pasos 1 al 3

Como se puede observar en la Figura 5, una transacción de Blockchain inicia cuando un usuario (Usuario 1) desea adquirir algún activo digital, por ejemplo, Smart Contracts, criptomonedas, entre otros, mediante la cual se inserta la información necesaria para que esta pueda llegar a su destinatario. Toda esta información posteriormente se procede a ser almacenada en forma de bloque para que pueda ser procesada, en donde, se junta con otras transacciones las cuales también ingresan a la

Blockchain en forma de bloques como se puede observar en la ilustración.

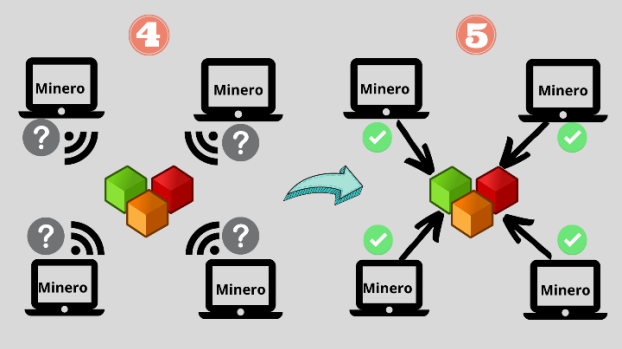

Figura *6*. Funcionamiento Blockchain - Paso 4 y 5

Una vez todas las transacciones han sido encapsuladas en forma de bloque, se procede a enviar a los diferentes nodos que componen la red interna de Blockchain ya que estos serán los encargados de verificar la validez de las transacciones que están por ser añadidas definitivamente al libro mayor de la cadena de bloques. Es por ello que para realizar esta verificación los mineros (Como se muestra en la Figura 6) son los encargados de realizar dicha verificación a través de los métodos de conceso los cuales fundamentan sus resoluciones con ayuda de cálculos matemáticos manteniendo las reglas de consenso que tiene cada método. Una vez se corrobora que todos los parámetros son correctos, los mismos mineros se encargar de dar la aprobación y la transacción se añade exitosamente a la cadena de bloques. Un dato importante en esta parte del procedimiento es que para que exista una aprobación exitosa es necesario que más del 50% de los mineros aprueben la transacción, caso contrario se deniega la adicción y se termina el procedimiento para ese requerimiento.

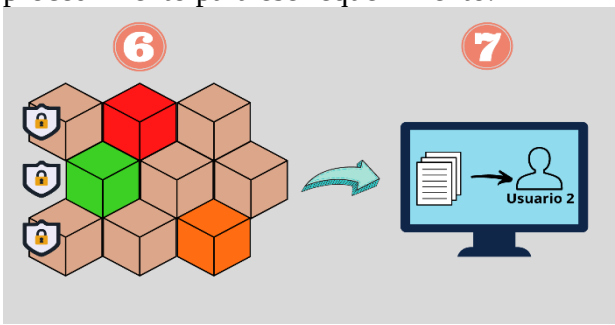

Figura *7*. Funcionamiento Blockchain - Paso 6 y 7

Si se observa la Figura 7, se puede apreciar que después que se añaden todas las transacciones aprobadas a la cadena de bloques, el siguiente paso en el procedimiento es la aplicación de medidas criptográficas con las cuales se garantiza que éstas no puedan ser alteradas por ningún motivo, manteniendo la confidencialidad de los datos y los usuarios involucrados. Finalmente, la transacción es recibida por el destinatario (Usuario 2) al cual se le entrega su activo digital solicitado respectivamente, dando por concluida la transacción de manera correcta.

4.4. Aplicaciones

El principal crecimiento de Blockchain se ha dado por la facilidad con la cual puede ser implementada en varios ámbitos, es por esta razón que a continuación se presenta algunos casos en donde se ha optado por la utilización de esta tecnología para mejorar sus aplicativos y, a su vez, obtener mejores resultados. Por lo tanto, se presenta a continuación algunos de estos.

4.4.1. Salud

En cuanto al ámbito de la salud esta tecnología ha sido utilizada para almacenar las historias clínicas de los pacientes, con la finalidad de mejorar el manejo de los datos delicados de un hospital. Es por ello que se considera que “Blockchain tiene el potencial de poner la gestión y transmisión de datos médicos en manos de los pacientes directamente, de modo que el historial médico se mantiene y se puede buscar, y solo los proveedores de atención autorizados pueden verlo y almacenarlo” [20]. garantizando de esta manera la seguridad y confidencialidad de la información importante de las entidades de salud.

4.4.2. IoT: Internet de las cosas

La combinación entre IoT y Blockchain ha sido de gran utilidad para la implementación de lo que se conoce actualmente como las Smart City ya que como se menciona en la mayoría de casos, esta tecnología se caracteriza por asegurarse en primer plano de mantener seguras sus conexiones y los datos que se almacena en

ella es por esto que "La integración de la tecnología IoT y Blockchain hace que el sistema sea robusto y a prueba de manipulaciones" [4]. esto quiere decir que se presenta un modelo de seguridad de carácter descentralizado, lo cual permite tener un mayor control ya que este esquema tiene la ventaja de ser más escalable a diferencia de un sistema centralizado.

4.4.3. Legal

En el apartado legal, esta tecnología aparece como la alternativa para manejar contratos legales de cualquier tipo, con la eventualidad que reduce considerablemente la intervención del ser humano evitando de esta manera divulgaciones, o en casos más extremos, la modificación de esos contratos, ya que al ser un software el que se encarga de realizar las verificaciones, si una de estas no es acatada correctamente el sistema automáticamente procederá a lanzar una advertencia con la cual se alerta a todos los involucrados del problema y, además, detendrá cualquier movimiento de lectura y escritura del documento legal digital que se encuentra almacenado en la cadena de bloques.. De esta manera, Blockchain "puede ser una solución para los marcos legales actuales que regulan los contratos entre jurisdicciones para mantener un libro de contabilidad digital sin el tercero" [4].

En consecuencia, esto ayuda a conservar de una manera más adecuada la seguridad y privacidad del usuario normal que interviene en estos procesos.

4.4.4. Financiero

Cuando se habla de Blockchain por lo general suele ser relacionado con lo monetarios ya que su auge surgió gracias a las criptomonedas en un principio, por esta razón, su impacto en el ámbito financiero es indiscutible lo cual ha provocado que sea utilizado con mayor frecuencia ya que al ser considerado un libro contable universal en el cual no se requiere de la intervención de un tercero para realizar una transacción monetaria entre dos usuarios, esto facilita el control de los activos que se están enviando, asi como de su pago respectivo, reduciendo considerablemente los costos operativos y de personal, ya que al no necesitar de la mano humana, se automatizan los procesos y se obtienen resultados más eficaces y seguros. Por lo tanto, los autores Mela y Cedeño, indican una concepción al respecto, en donde, "Blockchain en el sector financiero tiene mucha utilidad, ya que, brinda su mayor ventaja y su finalidad es mantener seguro los procesos que se realicen a nivel económico, claramente, tomando en cuenta las diferentes capas de la estructura que tiene la cadena de bloques" [21].

De esta manera permite que tanto empresarios pequeños como grandes corporaciones puedan expandirse en el mercado local e internacional y, en su defecto, puedan transformar su negocio proporcionando servicios avanzados.

4.4.5. Big Data

Al manejar datos es importante mantenerlos almacenados adecuadamente para evitar consecuencias graves a futuro, es por esta razón y otras más que aparece como alternativa la inclusión de Blockchain ya que esta presenta una variedad de métodos mediante los cuales se puede manipular la información. Por lo tanto, se controla mediante la Blockchain que cada acción que comprometa la integridad de los datos se pueda observar de manera transparente por parte de los demás usuarios, manteniendo en todo momento la seguridad de estos. Sin embargo, según los autores Dolader, Bel y Muñoz consideran que "los datos podrían ir acompañados de pruebas de integridad a bajo nivel o incluso, en el caso de la extracción, de firmas concretas que posibiliten su trazabilidad" [22].

De esta manera la relación de Big Data con Blockchain ha ido evolucionando con el paso del tiempo, tanto que se ha producido varias combinaciones entre estas, dando como resultado, aplicativos de gran prestigio, así como el caso de Kiyomoto el cual "diseñó una plataforma de comercio de datos distribuidos basada en blockchain que aprovecha Hyperledger, en la que los nodos actúan como

intermediarios, receptores y verificadores de datos" [23].

4.4.6. Educativo

En cuanto a lo académico la implementación de Blockchain pasó desapercibida en los años anteriores ya que no se le veía mayor utilidad para el sistema educativo. Sin embargo, con la aparición de la pandemia de la actualidad, tomo más fuerza en algunas partes del mundo el uso de esta tecnología para la entrega de documentos académicos de manera digital, es decir, la entrega de certificados con firmas criptográficas que garantizan la validez de estas y puedan ser recibidas por el usuario de manera segura. Por esta razón, nace el termino Blockcerts el cual "es un conjunto de estándares desarrollados para que los participantes emitan y verifiquen registros académicos, trabajando con cualquier blockchain. Se basa en un trabajo conjunto realizado en el MIT Media Lab y en Learning Machine" [24].

Sin embargo, en sus inicios esta aplicación fue basada en la arquitectura que maneja actualmente el Bitcoin en donde se promovía un rendimiento adecuado, pero para mejorar la experiencia de ésta, poco tiempo después fue reforzada por la cadena de bloques de Ethereum, con la cual se añadía el beneficio de la detección fallos en el aplicativo. Pero a pesar de que esta aplicación mantiene lo mejor de la tecnología Blockchain, al ser bastante estricta en cuanto al manejo de la información, "tiene el problema de ser extremadamente crítico cuando el usuario tiende a usarlo, lo que significa que un error cometido con la aplicación obligará al usuario a revocar; lo cual requiere el permiso del propietario y del emisor" [25].

5. DISCUSIÓN

Como se puede observar Blockchain con el pasar del tiempo ha sido incluido en varias aplicaciones en diferentes ámbitos pero a pesar de esto, aún se mantiene el cuestionamiento sobre la rentabilidad de utilizar Blockchain, por esta razón se ha decidió realizar un análisis FODA en el cual se pude apreciar tanto las ventajas como las desventajas que puede tener en general Blockchain, ya que de esta manera se entrega al usuario un punto de vista diferente con respecto a la cadena de bloques, facilitando así la toma de decisiones para futuros usuarios cuando piensan en utilizar una arquitectura basada en esta tecnología, con el fin de conocer todas las implicaciones que esta puede tener y el impacto en su aplicativo.

Sin embargo, para realizar dicho análisis es necesario considerar los puntos críticos analizados en el artículo en donde se empieza por su concepto donde a breves rasgos nos muestra una tecnología bastante llamativa, que tiene como fortaleza principal la de mantener estrictas reglas de seguridad en los datos que almacena en su interior. En consecuencia, nace la curiosidad de cómo logra este objetivo Blockchain, en donde se obtiene como resultado el análisis respectivo a sus elementos, con los cuales se aclara la idea del funcionamiento que tiene blockchain, por lo tanto, se tiene un enfoque más definido sobre cuáles pueden ser los beneficios y falencias que se pueden presentar cuando se implementa una cadena de bloques como fuente principal para que los procesos se ejecuten correctamente. En la figura 8 se puede observar el FODA respectivo teniendo en cuenta los diferentes aspectos fueron considerados para la investigación.

Fortalezas	Debilidades
• Mantiene un sistema de red descentralizada. • La información es transparente para todos los usuarios. • Registra cualquier evento considerado importante para la cadena de bloques. • Mantiene la privacidad en todas las transacciones.	• Es imposible realizar una recuperación de cuenta, en caso de perdida, debido a su rígida seguridad. • Variación de velocidad en el procesamiento de una transacción. • No tiene un ente regulador.
Oportunidades	**Amenazas**
• Crecimiento de pequeñas empresas en el mercado internacional. • Reducción de costos operativos en mantenimiento de aplicativos	• Existencia de usuarios con malas intenciones dentro de la cadena de bloques. • Libre albedrio al momento de decidir sobre la validez de una transacción • Lavado de activos por parte de entidades fraudulentas.

Figura *8*. Análisis FODA de Blockchain

6. CONCLUSIONES

Blockchain ha tenido un impacto significativo en cuanto al desarrollo que mantiene la tecnología con el pasar del tiempo, es por ello que en el presente estado del arte se evidencia las características más importantes que hacen que éste sea considerado como algo esencial para el desarrollo de varios ámbitos en los cuales no se creía posible que se puede digitalizar o, en su defecto, tener la confianza de que una tecnología nueva pueda tener una efectividad bastante prometedora manteniendo los estándares adecuados por los diferentes entes que utilizan en sus arquitecturas la cadena de bloques.

Las metodologías de revisión sistemática nos han permitido que el desarrollo de la investigación tome un orden respectivo, en donde prevalece la calidad de los datos que fueron seleccionados para ser incluidos en la investigación, dando como resultado, información relevante con respecto a Blockchain, puntualizando en los diferentes apartados que se consideraron en el trabajo investigativo con la finalidad de entregar un estado del arte con la información más actualizada con respecto a esta

Con respecto a Blockchain al ser analizada por varios autores puede llegar a tener varios puntos de vista pero todos éstos se caracterizan por tener un punto de similitud en particular y es el de ser una tecnología en la cual no es necesario la intervención de un tercer usuario para que pueda funcionar adecuadamente, ya que los mismos usuarios que intervienen en su red son los encargados de otorgar autorizaciones para la ejecución adecuada por medio de un consenso mutuo entre todos, garantizando de esta manera la transparencia de los procesos internos que se realizan en la cadena de bloques.

Sin embargo, para que todo esto sea posible, existen una serie de elementos que interviene para que Blockchain puede desarrollar sus procesos efectivamente, los cuales, se analizan desde el más primitivo que es el usuario que es capaz de crear una transacción en cualquier parte del mundo, hasta el más complejo el cual es la Criptografía y los métodos de consenso con los cuales se asegura que la transacción pueda ejecutarse con toda la seguridad del caso y sea revisada por todos los mineros para que posteriormente puedan ser añadidos a la cadena de bloques sin mayor problemas. Por lo tanto, el funcionamiento de Blockchain dependerá del correcto desarrollo de cada elemento en cada etapa que concierne a las transacciones entre dos usuarios que se encuentran en lugares diferentes.

Pero al ser una tecnología la cual es considerada de código abierto y de libre modificación por parte de los usuarios que conocen del tema, se convierte en un procedimiento que puede ser usado de manera contraproducente ya que se ha evidenciado que se puede llegar a privatizar hasta cierto punto la blockchain, lo cual provoca que exista una persona encargada de mantener el control de las transacciones que se realizan en esa organización, quitándole en su gran mayoría la principal característica de la cadena de bloques la cual es la descentralización, ya que aplicar estas reglas privadas se convierte un sistema centralizado lo cual limita a los usuarios a tener acceso a ciertos datos y ser restringidos de realizar cualquier actividad que no esté permitida por la entidad que administra el sistema, debilitando la confidencialidad y viabilidad del aplicativo basado en esta tecnología. De esta manera, se sabe que Blockchain puede ser inmiscuida en varios ámbitos, sin embargo, su resultado será variable dependiendo de cada caso de aplicación.

Es por ello que se ha puesto en evidencia un análisis FODA con respecto a Blockchain en donde, se observa las diferentes implicaciones que tiene al momento de ser considerada para su implementación o combinación para un sistema existente teniendo en cuenta que tanto las ventajas como desventajas de este, las cuales son bastante criticas ya que puede tener resultados positivos si le lo usa con las medidas del caso, pero como se mencionó anteriormente, si llegase a manos equivocadas la decisión de un

transacción en la cadena de bloques, puede provocar que exista algún tipo de fraude y la perdida de activos digitales, sin rastro del culpable del hecho puesto que al ser anónimo los usuarios de la red, encontrar un culpable del hecho se vuelve casi imposible.

7. REFERENCIAS

[1] F. J. Quesada Real, «Repositorio de Trabajos Académicos de la Universidad de Jaén,» Junio 2019. [En línea]. Available: http://tauja.ujaen.es/bitstream/10953.1/11599/1/QUESADA_REAL_FRANCISCO_JOSE_TFM_INFORMATICA.pdf. [Último acceso: 15 Agosto 2021].

[2] J. Liu, S. Peng, C. Long, L. Wei, Y. Liu y Z. Tian, «ACM - Digital Library,» 12 Marzo 2020. [En línea]. Available: https://bibliotecas.ups.edu.ec:3396/doi/pdf/10.1145/3390566.3391681. [Último acceso: 28 Julio 2021].

[3] R. A. M. López, «Repositorio - Universidad de León,» 4 Junio 2018. [En línea]. Available: https://buleria.unileon.es/bitstream/handle/10612/8566/Raul%20Andr%C3%A9s%20Marqu%C3%A9s%20L%C3%B3pez%20TFGADE_julio18.pdf?sequence=1. [Último acceso: 27 Junio 2021].

[4] B. K. Mohanta, D. Jena, S. S. Panda y S. Sobhanayak, «ScienceDirect,» 07 Septiembre 2019. [En línea]. Available: https://bibliotecas.ups.edu.ec:2230/science/article/pii/S2542660518300702. [Último acceso: 01 Noviembre 2021].

[5] P. Brereton, B. A. Kitchenham, D. Budgen, M. Turner y M. Khalil, «ScienceDirect,» 17 Agosto 2006. [En línea]. Available: https://www.sciencedirect.com/science/article/pii/S016412120600197X. [Último acceso: 20 Agosto 2021].

[6] K. Petersen, S. Vakkalanka y L. Kuzniarz, «ScienceDirect,» 28 Marzo 2015. [En línea]. Available: https://bibliotecas.ups.edu.ec:2230/science/article/pii/S0950584915000646. [Último acceso: 20 Agosto 2021].

[7] K. Petersen, R. Feldt, S. Mujtaba y M. Mattsson, «ACM - Digital Library,» Junio 2008. [En línea]. Available: https://dl.acm.org/doi/10.5555/2227115.2227123. [Último acceso: 24 Agosto 2021].

[8] J. M. L. Moreno y C. R. Herrero, «ResearchGate,» Marzo 2018. [En línea]. Available: https://www.researchgate.net/publication/323540481_Cutrecoin_como_programar_una_criptodivisa_desde_cero_y_no_morir_en_el_intento. [Último acceso: 25 Junio 2021].

[9] T. W. Kim y A. Zetlin-Jones, «ResearchGate,» 28 Agosto 2019. [En línea]. Available: https://www.researchgate.net/publication/335482881_The_Ethics_of_Contentious_Hard_Forks_in_Blockchain_Networks_With_Fixed_Features. [Último acceso: 26 Junio 2021].

[10] F. Schär, «ResearchGate,» Febrero 2020. [En línea]. Available: https://www.researchgate.net/publication/339461094_Blockchain_Forks_A_Formal_Classification_Framework_and_Persistency_Analysis. [Último acceso: 26 Junio 2021].

[11] H. Acuña, «ESE - Universidad de los Andes,» 15 Agosto 2017. [En línea]. Available: https://www.ese.cl/ese/site/artic/20180514/asocfile/20180514111252/bitcoin_y_criptomonedas.pdf. [Último acceso: 27 Junio 2021].

[12] J. Suárez, «Repositorio - Universidad del País Vasco,» 2020. [En línea]. Available: https://addi.ehu.es/bitstream/handle/10810/48832/TFG___Julen.pdf?sequence=2&isAllowed=y. [Último acceso: 27 Junio 2021].

[13] R. Bhatia, P. Kumar, S. Bansal y S. Rawat, «IEEE Xplore,» 22 Junio 2018. [En línea]. Available: https://bibliotecas.ups.edu.ec:2095/stamp/stamp.jsp?tp=&arnumber=8441738. [Último acceso: 27 Junio 2021].

[14] C. Mohan, «ACM - Digital Library,» 25 Junio 2019. [En línea]. Available: https://bibliotecas.ups.edu.ec:3396/doi/10.1145/3299869.3314116. [Último acceso: 30 Junio 2021].

[15] J. Polge, J. Robert y Y. Le Traon, «ScienceDirect,» 12 Septiembre 2020. [En línea]. Available: https://doi.org/10.1016/j.icte.2020.09.002. [Último acceso: 30 Junio 2021].

[16] L. Parrondo, «Tecnología blockchain, una nueva era para la empresa,» *Revista de Contabilidad y Dirección: Blockchain, bitcoin y criptomonedas,* vol. 27, pp. 11-31, 2018.

[17] Z. Li y L. Zhang, «ACM - Digital Library,» 14 Abril 2020. [En línea]. Available: https://bibliotecas.ups.edu.ec:3396/doi/pdf/10.1145/3397125.3397153. [Último acceso: 05 Agosto 2021].

[18] T. Q. Ban, B. N. Anh, N. T. Son y T. V. Dinh, «ACM - Digital Library,» 19 Febrero 2019. [En línea]. Available: https://bibliotecas.ups.edu.ec:3396/doi/pdf/10.1145/3316615.3316671. [Último acceso: 05 Agosto 2021].

[19] B. Y. Navarro, *Blockchain y sus aplicaciones,* Articulo de Investigacion: UC Asuncion (Paraguay), 2017.

[20] F. J. Quesada Real, «Repositorio de Trabajos Académicos de la Universidad de Jaén,» Junio 2019. [En línea]. Available: http://tauja.ujaen.es/bitstream/10953.1/11599/1/QUESADA_REAL_FRANCISCO_JOSE_TFM_INFORMATICA.pdf. [Último acceso: Agosto 2021].

[21] J. L. Mela N. y E. J. H. Cedeño, «ResearchGate,» Diciembre 2019. [En línea]. Available: https://www.researchgate.net/publication/338335642_Tecnologias_Blockchain_y_sus_aplicaciones. [Último acceso: 02 Novimebre 2021].

[22] C. R. Dolader, J. R. Bel y J. L. T. Muñoz, «La Blockchain: Fundamentos, Aplicaciones Y Relación Con Otras Tecnologías Disruptivas,» *Revista Economía Industrial,* pp. 33-40, 2017.

[23] W. Gao, W. G. Hatcher y W. Yu, «IEEE Xplore,» 2018. [En línea]. Available: https://bibliotecas.ups.edu.ec:2095/document/8487348. [Último acceso: 02 Noviembre 2021].

[24] F. Vidal, F. Gouveia y C. Soares, «IEEE Xplore,» 2019. [En línea]. Available: https://bibliotecas.ups.edu.ec:2095/document/8945824. [Último acceso: 02 Noviembre 2021].

[25] A. El-Dorry, M. Reda, S. A. E. Khalek, S. E.-D. Mohamed, R. Mohamed y A. Nabil, «ACM - Digital Library,» Noviembre 2020. [En línea]. Available: https://bibliotecas.ups.edu.ec:3396/doi/10.1145/3436829.3436864. [Último acceso: 02 Noviembre 2021].