Recibido: May. 23, 2023 | Aceptado: Jul. 28, 2023 | Publicado: Ago. 14, 2023

Utilización de las Criptomonedas e Integridad de Blockchain

Use of Cryptocurrencies and Blockchain Integrity

DOI: https://doi.org/10.21803/ingecana.3.3.637

Luis Alejandro Avellaneda Vásquez[1] y Angel Alberto Varón Quimbayo[2]

1.Ingeniería de Sistemas, Fundación Universitaria del Área Andina. lavellaneda7@estudiantes.areandina.edu.co, https://orcid.org/0009-0004-3106-6384.

2. Magíster Universidad Internacional Iberoamericana de Puerto Rico, Docente Fundación Universitaria del Área Andina. Email: Avaron2@areandina.edu.co, Orcid: https://orcid.org/0000-0003-0643-358X.

Resumen

Actualmente se habla mucho de la tecnología Blockchain, porque brinda herramientas enfocadas a proporcionar el funcionamiento de nuevas tecnologías, tanto financieras que brindan transparencia y confianza a la ciudadanía en la vida cotidiana y su viabilidad en proyectos diferentes a las criptomonedas como son contratos inteligentes (Smart Contracts), con los cuales se pueden racionalizar los pasos en un negocio al ser llevados a cabo, auditados por un tercero neutral y sin corrupción generada por un interés. Además, exponer técnicas de seguridad que permitan mitigar el conflicto de la seguridad informática, siendo amigables con el usuario que se encuentre interesado en incursionar en el mundo digital, inherente a esta tecnología. este artículo, expone un análisis sobre la funcionalidad de la cadena de bloques y las herramientas que utiliza esta tecnología, para brindar servicios a las organizaciones, para ello se acude al método de investigación documental, extrayendo información de documentos desarrollados por expertos, sobre temática en mención, y que permita el desarrollo de la investigación. Por lo tanto, se concluye que Blockchain llegó para quedarse, bajo esta premisa exige que las organizaciones se atrevan a innovar en sus procesos financieros y que incluyan las criptomonedas como elemento de negocio.

Palabras clave: Blockchain; Criptomoneda; Ethereum; Mineros.

Abstract

Currently there is much talk about Blockchain technology, because it provides tools focused on providing the operation of new technologies, both financial that provide transparency and confidence to citizens in everyday life and its viability in projects other than cryptocurrencies such as smart contracts (Smart Contracts), with which you can streamline the steps in a business to be carried out, audited by a neutral third party and without corruption generated by an interest. In addition, expose security techniques to mitigate the conflict of computer security, being friendly to the user who is interested in venturing into the digital world, inherent in this technology. This article presents an analysis of the functionality of the blockchain and the tools used by the blockchain, to provide services to organizations, for it goes to the documentary research method, extracting information from documents developed by experts, on the subject in question, and that allows the development of research. Therefore, it is concluded that Blockchain is here to stay, under this premise requires that organizations dare to innovate in their financial processes and include cryptocurrencies as a business element.

Keywords: *Blockchain; Cryptocurrency; Ethereum; Miners.*

Cómo citar este artículo:

L. A. Avellaneda-Vásquez, A. A. Varón-Quimbayo, «Utilización de las Criptomonedas e Integridad de Blockchain». Ingente Americana, vol. 3, n°3, e-637, 2023. DOI: https://doi.org/10.21803/ingecana.3.3.637.

Introducción

Uno de los mayores inconvenientes con la incorporación de divisas virtuales para el uso común en el territorio nacional, es que el Banco de la República Colombiano no ha reglamentado su curso y la mantiene en un limbo donde no es legal. [1]

Como referente se puede tomar el caso de el Salvador que en 2021 el gobierno adquirió 2 punto 301 Bitcoin, para convertirla en la moneda de circulación de ese país, todo esto permitió que llegaran inversionistas extranjeros y se interesaron en la economía del Estado, aunque se ha visto un descenso del valor que mostraba durante la pandemia. [2] [3]

En Colombia en el proyecto Nvio Pagos Colombia S.A.S ambicioso de la empresa Bitso en conjunto con la superintendencia financiera, han comenzado un piloto para la inversión en Criptomonedas probando la efectividad de esta divisa y así aumentar la competitividad a nivel internacional, para llamar la atención de los inversionistas locales en el medio descentralizado. [4]

La información obtenida presenta un panorama posiblemente alentador sobre la implementación de Criptomonedas, sin embargo, es un tema a revisar por la fluctuación del valor nominal del Bitcoin que sería la moneda base a tener en cuenta.

MARCO TEÓRICO

¿ASPECTOS TEÓRICOS SOBRE BLOCKCHAIN?

Es una cadena de bloques de comunicación, no centralizada que se transmite entre nodos con firma electrónica, que se vale de funciones Hash y los árboles de Merkle, en pro de mantener la triada de la información. [5]

Blockchain también es contemplado como un almacén de datos direccionado como libro público, participativo al incorporar distintos usuarios que introducen todo tipo de información, estos registros van a la Base de Datos contenidos en cada nodo de la red, amparados por sistemas criptográficos que admiten que el acceder a los datos se dé únicamente por medio de contraseña encriptada, y se genere y guarde una copia igual en la secuencia, esto avala la protección y disponibilidad de datos constante, lo que ofrece seguridad al admitir generar, modificar, asignar y guardar los datos, ya que la cadena de bloques se encuentra determinado por algoritmos matemáticos brindando confiabilidad al usuario, esta tecnología disruptiva es versátil, se puede emplear en diferentes espacios como: el arqueo de costes, aseguradoras y servicios bancarios, trámites de registros e inversiones". [6]

Blockchain se traduce como cadena de

bloques que implica una práctica informática o protocolo, inicialmente generada con la intención de soportar las criptomonedas cuyo paradigma es Bitcoin; la cual presenta dos caracteres distintivos básicos, respecto a la moneda habitual a saber:

Según los efectos propios, el ámbito descentralizado y la disrupción que sugiere en vías de pago, en el ámbito económico; radica en que las criptomonedas, por lo general, han procedido al margen de monedas fiduciarias. Se puede evidenciar que los valores relacionados con las mismas se hallan potentemente fijadas por la ley de oferta/demanda. Blockchain es la base de Bitcoin, lo que significa que este protocolo sistemático sirve de soporte a la criptomoneda más valiosa actualmente. [7]

Algunas características de Blockchain son su transparencia, fiabilidad, y seguridad, supervisión por parte de los usuarios que se encuentren en la Red, están enfocados al internet de las cosas en el seguimiento de mercancías que se transportan, manejo de inventarios debido a su inmutabilidad, y el uso de criptomonedas, también cuenta con la posibilidad del manejo de grandes cantidades de datos (Big Data), dirigidas a las cadenas de bloques para incrementar la seguridad. [6]

Por esta razón se utilizan métodos Hash que son funciones de resumen criptográfico unidireccional, que contiene un algoritmo matemático; cuando hay un bloque de datos en un lenguaje común con destino a la Blockchain son procesados por la función Hash, para ser transformados en un nuevo formato con una longitud de caracteres fija, donde un bloque de la cadena contiene los datos del bloque anterior en una lista enlazada y a través de aritmética modular se verifica la integridad de los datos, ya que si han sido modificados no encajaran con los otros elementos de la Blockchain. [5]

El árbol de Merkle es una estructura de funciones Hash propuesta por Ralph Merkle en 1979, que parte de un nodo raíz a un nodo padre, que puede tener 2 nodos hijos y los nodos que no tienen hijos son nodos hoja que contienen datos arbitrarios, mientras que los nodos padres contienen los datos de sus dos nodos hijo en conjunto, esto se realiza con el fin de facilitar el trabajo y buscar una información, ya que debe basarse en el logaritmo del número de nodos hoja de una estructura de árbol. [5]

Referente a la tecnología de contabilidad distribuida

DLT (Distributed Ledger Technology) es un libro donde se guarda la contabilidad y movimientos realizados de la Blockchain referente a Criptomonedas, replicado para cada nodo inmanipulable sin el permiso de los otros nodos y así evitar que el valor de una transferencia pueda ser usado una segunda vez, antes del visto bueno del receptor. [8]

Otro mecanismo criptográfico que utiliza esta tecnología es la firma electrónica, que es concebida como un procedimiento que usa el certificado digital para firmar documentos, asegurando su autenticidad y autoría. Normalmente usa el sistema de cifrado asimétrico con una clave pública, generada a partir de la clave privada para el receptor y la clave privada para el emisor. En el caso de Blockchain para Criptomonedas, se usa un cifrado asimétrico ECDSA (Algoritmo de firma digital de curva elíptica), con una curva elíptica de Koblitz secp 2561. [5]

De igual manera esta tecnología aplica un algoritmo de firma digital de curva elíptica más conocido como ECDSA (Elliptic Curve Digital Signature Algorithm)

Similar al criptosistema asimétrico, ya que requiere que los pares de claves privadas/

públicas utilizados para la generación y verificación de firmas digitales, se generen con respecto a un dominio determinado. Se comienza con una combinación aleatoria de 256 bits como clave privada, basándose en esta se deriva en una clave pública de 65, además durante la generación de los parámetros de dominio se requiere una función hash aprobada. Y con la clave pública que cumpla con los parámetros, se obtiene el seudónimo de un usuario mediante las funciones resumen SHA-256 y RIPEMD-160. Bits [5] [9]

FUNDAMENTACIÓN TEÓRICA DE LAS CRIPTOMONEDAS

Las criptomonedas son una forma de dinero creado sobre una elegante base tecnológica que aporta seguridad, comodidad e inmediatez, entre otros beneficios fundamentales, es decir son activos encriptados, por lo que es significativo e interesante hacer un breve recorrido a través de la relación con el dinero desde sus formas más primitivas para llegar a entender su concepción, con ello, tanto el potencial de Blockchain y las criptomonedas como su aplicación financiera. [8] [10]

Actualmente, existen más de 3800 criptomonedas, una de ellas es Bitcoin constituyéndose como la más conocida, comienza el 31 de octubre del 2008 con Satoshi Nakamoto, es el apelativo del usuario creador que comenzó un proceso de comunicación peer-to-peer con otros usuarios en la red. [8]

Para enero de 2009, Satoshi Nakamoto realizó la primera transacción de Bitcoin específicamente 10 a un estrecho amigo Hal Finney, a finales del 2009; en noviembre Satoshi Nakamoto por medio de un foro en Bitcointalk daba la bienvenida a nuevos usuarios, para que fungieron como nodos de transacciones además de mineros que generen nuevas monedas y así aumentar la cantidad de Bitcoin disponibles. [8]

Para apoyar la seguridad de los crecientes usuarios, al realizar transacciones se usa la firma digital oculta, donde por medio de cifrado asimétrico se hace llegar a un tercero el documento de la transacción para que lo firme como validador de la transacción realizada, pero este tercero no tendrá acceso a la información dentro de la transacción. Si este modo no fuera usado, el dinero no se debitará de la cuenta y seguiría estando disponible hasta que el receptor diera el visto bueno a la transacción. [8]

Además, el Bitcoin nace como una protesta de los Chyperpunks activistas informáticos, que incentivan el uso de criptografía a los bancos tradicionales incitado principalmente por la crisis de la burbuja inmobiliaria del 2008 en Estados Unidos, debido a la privacidad que ofrecía el Bitcoin y la independencia a entidades y bancos estatales. En su línea histórica se destacan tres momentos desde el 2007 hasta mediados del 2011 donde se desarrolla la tecnología Bitcoin por Satoshi Nakamoto y se maneja en un nicho reservado de informáticos avanzados. [5]

A finales del 2011 y hasta 2015 Bitcoin se gana una mala fama, debido a que al anonimato que brinda la plataforma sujetos u organizaciones lo usan con fines fraudulentos, más sin embargo en 2015 representantes del mundo financiero analizan más a fondo la tecnología base Blockchain y descubren que puede ser de utilidad, para proyectos financieros entre los que destaca M-Pesa plataforma de banco impulsada por la compañía BitPesa del 2013. [5]

Por lo tanto, los nodos son un Software de código abierto en una Red P2P autárquico de entidades punto a punto con usuarios al mismo nivel a tiempo real, en donde se manejan consensos entre nodos para realizar acciones en el cuál ninguno puede manejar la forma de comunicación ni tomar el control de la operación autónomamente y todos guardan una copia de

seguridad parcial o total de las transacciones. [8]

Para la aprobación de estas transacciones se recurre a los mineros que son nodos que optan por la tarea de realizar la verificación de las transacciones realizadas con una operación matemática math.pow (método para retornar un número especificado elevado a la potencia determinada), la cual retorna la base elevada al exponente, es decir, base exponente. [8]

La base y el exponente están en el sistema numérico decimal agregadas a un bloque con destino a la Blockchain a través de una verificación de los nodos buscando que la información plasmada sea verídica, después de verificar que los datos son ciertos se compite por descifrar el mensaje de la transacción, validarlo y cifrarlo nuevamente, para llevarlo a consenso y si es positivo el minero obtiene una recompensa de 12,5 Bitcoins como incentivo por plasmarlo en la DLT (tecnología de contabilidad distribuida), escribir el bloque final y agregarlo oficialmente a la Blockchain generando una copia para los otros nodos. [8]

A. Los contratos inteligentes y Ethereum

Contratos inteligentes es un concepto expuesto por Nick Szabo en 1994, como una metodología que usa programación como componente inteligente en lenguaje de IDE (Entornos de Desarrollo Integrado), Solidity y serpent con cláusulas entre las partes acorde a las acciones solicitadas similar a un contrato tradicional, el auge de la idea de Szabo se da con la aparición de Bitcoin por Satoshi Nakamoto. [8] [11] Además de su implementación a la tecnología Blockchain también se da su mayor aplicabilidad en el sector médico, administrativo y/o electoral, donde cumple con tres principios fundamentales que son: revisión por medio de una red de ordenadores que lleguen al consenso de su ecuanimidad, cumplir con funciones criptográficas resumen y verificación de que más de la mitad de los ordenadores que forman parte del consenso sean honestos, para mantener la inmutabilidad de los contratos inteligentes plasmados en la tecnología de contabilidad distribuida. [8] [11]

Si bien Bitcoin es un contrato inteligente sencillo debido a la tecnología Blockchain en su programación sigue siendo limitado, es donde surge Ethereum con su lenguaje de programación Solidity, debido a la necesidad de una divisa virtual que soporte la implementación de contratos inteligentes, se conforma de usuarios con cuentas no permisionadas y billeteras virtuales (Ethereum-Wallet, MetamMask y MyEtherWallet). [5]

Esta herramienta se usa para gestionar los fondos, aunque también se pueden usar aplicaciones descentralizadas llamadas DApps que conectan directamente a los usuarios sin intermediarios, para que puedan cerrar tratos accesibles a través de navegadores web 3.0 (Mist, Parity) [5]

Estas Dapps son diseñadas específicamente para ello, ya que sus funciones están fuera de la jurisdicción de las billeteras virtuales e interactúan directamente con los procedimientos de la Blockchain y los contratos inteligentes, como un nodo completo con una copia de seguridad de cada archivo. [5]

La gestión se hace usando nodos ligeros con una versión resumida de los archivos o un nodo sencillo sin funcionalidades de alto nivel, los tres funcionando como cartera virtual; existe la posibilidad de crear redes privadas entre nodos específicos en una red con cifrado asimétrico, basado en curvas elípticas que pueden crear varios pares de claves privadas que sirven para generar la firma digital y la clave pública que comparten para verificar la firma digital; más

sin embargo, cada clave tendrá trazabilidad para garantizar el pseudo anonimato. [5]

Por otro lado cabe mencionar el Ether que es la moneda del entorno Ethereum usada para realizar las operaciones en la red con comandos en el lenguaje Solidity propio de esta plataforma que consume recursos y ocupan espacio de los nodos, igual a cuando se va a agregar un valor nuevo a la Blockchain, por lo que para incentivar la participación de los nodos y un reparto equitativo de las recompensas surge la noción de gas, un catálogo de valores definidos para cada fragmento de programación y almacenamiento requeridos para la operación, esta puede ser usada para realizar transacciones con transmisión de valor o la creación y/o ejecución de un contrato inteligente. [5]

Siguiendo con este razonamiento las transacciones con transmisión de valor, se componen de una dirección de origen que es la cuenta de usuario identificada como el comienzo de la llamada que genera un contrato inteligente, además el primer contrato inteligente puede generar un segundo contrato inteligente usando una dirección obtenida a partir de diversos valores públicos, al desplegar el primer contrato inteligente y así sucesivamente. [5]

A diferencia del origen el contrato inteligente que genere otro sucesivamente, es un emisor del mensaje identificado como el anterior al contrato inteligente generado, cuando se ha culminado este primer paso debe identificarse un destinatario con la dirección de usuario o la dirección de contrato inteligente, cada transacción creada tendrá un número de identificación secuencial asignada a una cuenta de usuario, se especifica el valor de Ether que se desea transferir, además como se ha explicado antes, toda operación tiene un consumo que deberá ser cubierto por el usuario origen con gas pero, el usuario origen puede negociar el precio que está dispuesto a pagar por cada unidad de gas, para reducir el gasto a costa del tiempo que demora la operación. [5]

Los contratos inteligentes contienen una dirección procedente de una propiedad inherente de los mismos, en conjunto con variables globales como almacenamiento de nivel superior de la memoria del contrato, funciones públicas que es a lo que pueden acceder otros usuarios y compromisos inteligentes que lo llamen, contando también con funciones restringidas que son aquellas que responden exclusivamente a comandos dentro del contrato. [5]

En el caso de tratarse de la generación de un acuerdo nuevo, también debe tener en cuenta un balance, ya que al crear o llamar otros compromisos de este tipo tendrán un costo, para realizar estas operaciones deberá especificarse el código fuente del pacto para que pueda ser validado por los nodos en la red y genere otros, si se requiere recurrir a un contrato inteligente ya existente, se tendrán que anexar los parámetros de entrada. [5]

Además de esto, es importante saber que existe Una máquina virtual para Ethereum EVM (Ethereum Virtual Machine, que es un compilador intermedio entre el programador que usa el entorno de trabajo Solidity para ensamblar contratos inteligentes y el dispositivo que recibe los datos convertidos en Bytecode, que es el formato aceptado por la máquina final. La máquina virtual para Ethereum garantiza el determinismo del resultado final de todos los nodos, ya que, al tener un valor estándar para cada línea de código, se puede calcular la cantidad de gas necesario. [5]

B. Otras aplicaciones de Blockchain

NFT (No Fungible Token): Un Token no fungible, es un código único e irrepetible que se incorpora en un nuevo proyecto NFTracer, basada en Hyperledger Composer e Hyperledger, Fabric Blockchainy se compila a una Blockchain con el formato de

codificación hexadecimal común entre el Bitcoin, Ethereum y se espera que cumpla con la triada de la información, ya que contiene la identificación de un objeto incluyendo al propietario, no se puede dividir o cambiar por otros elementos similares al ser un identificador donde su naturaleza es demostrar la autenticidad del objeto para poder ser aplicado en contratos inteligentes, con el fin de realizar transferencias. [12] [13] Los ejemplos más claros son los bienes raíces y especialmente pinturas siendo aplicada en estos dos campos, al ser un fragmento de código que distingue los atributos de uno que va a ser transferido entre usuarios.

Existen dos modelos diferenciados los cuales son:

El modelo de arriba hacia abajo donde hay dos figuras, uno aplicando como propietario y subastador que se encarga de verificar que la información del archivo sea correcta, lo almacena en un bloque externo a una Blockchain existente, lo firma digitalmente para plasmarlo a un contrato inteligente y la otra figura actuando como comprador, verificando el convenio digital y confirmando la transacción.

La otra modalidad consiste de abajo hacia arriba, donde las dos figuras van a ser el creador de un NFT que diseña una plantilla de características básicas, para el objeto que va a ser subastado y agregado a un contrato inteligente además de un comprador que al momento de entrar a la puja puede personalizar algunas características adicionales acorde a una base de datos previamente predefinida, al ser culminada la transacción comienza la negociación por la compra y si es satisfactoria para las dos partes, se finaliza la transacción. [12] [13]

La particularidad radica en que no es una criptomoneda, sino sino que con estas se compra el título de propiedad de un objeto siendo este el NFT, más con el tiempo se valoriza el objeto en cuestión y es cuando se intercambia el título de propiedad NFT por un valor aumentado en criptodivisas al invertido inicialmente. [12] [13]

Otra herramienta es ICO (Initial Coin Ofering) que función es de inversión y se usa para obtener capital inicial a negocios emergentes que a diferencia del IPO (Initial Public Offering) en el que se ofertan acciones, ahora se ofrecen Tokens virtuales generados con la tecnología Blockchain a cambio de apoyo a la idea inicial. Esta nueva modalidad de ICO es atractiva, debido a las altas tasas de interés en retorno, aunque al ser un criptoactivo es extremadamente volátil y pueden presentarse prácticas delictivas al ser un bien descentralizado y fuera del alcance de entidades nacionales. [12][13]

Un dato importante sobre estos criptoactivos es que existen variaciones y a su vez híbridos entre estas variaciones, los criptoactivos más comunes son: El Criptoactivo de pago Currency Tokens, en el que se encuentran las monedas virtuales como medio de pago y deben almacenarse en una Hot Wallet o Cold Wallet; los criptoactivos de inversión Tokenized Securities basados en intereses obtenidos a partir de la ganancia y por último el Criptoactivo Utility Tokens, que le otorga al propietario acceso al servicio del negocio, un token similar es el Asset Tokens que otorga un activo físico o intangible, aunque el más famoso es el Tokenized Gold, que se especializa en operaciones con oro. [14][15]

Para enfatizar los beneficios de las ICOS se encuentran la descentralización e internacionalización, por lo que cualquier inversionista puede acceder a la oferta sin necesidad de recurrir a jurisdicciones gubernamentales en cuanto a negocios internacionales, además estos inversionistas serán usuarios y/o clientes del proyecto en su mismo inicio, al ser un sistema ilimitado, donde un inversionista puede acceder

a cualquier negocio sin necesidad de cumplir requisitos previos, también se encuentra la flexibilidad de medios que el emisor tiene para ofrecer recompensas al inversionista a diferencia del activo normativo, otro caso diferente al mercado de valores tradicional es la eliminación de la figura de intermediario necesario para acceder y ahora son regidos por un contrato inteligente más fiable al prescindir del factor humano. En el sistema a fondo que se basa en Blockchain donde se establece un consenso de todos los usuarios donde son los encargados de vigilar la seguridad en la Red realizando una trazabilidad de las operaciones realizadas y mantener un balance para no devaluar o revalorizar de más un valor, para mantener un equilibrio. [14][15]

Como en todo, es necesario observar los riesgos y para la materia de las ICOS también se encuentran representados en la falta de una legislación y regulación institucional, por lo que el usuario se encuentra fuera de la cobertura jurídica y se puede tornar en una tarea extensa e incluso tediosa convertir las criptodivisas en monedas como pueden ser el dólar o el euro al ser vistas como algo extraño e irregular. [15]

Además, como se mencionó una de las ventajas con las que se cuenta, es el control contable para manejar un equilibrio más; sin embargo, ese balance se basa en la especulación y puede mostrar ciertos momentos de flaqueza y dar un valor inexacto. [15]

También se encuentra la volatilidad de la idea de negocio al no existir un formato estándar para el desarrollo de la documentación inicial con las evidencias que sustentan el negocio que el emisor da a conocer al inversor que lo está patrocinando y por esto existe la posibilidad de que no se lleve a cabo el proyecto acorde al Whitepaper original o se cancele de facto y se incurran en pérdidas para el inversor, sin contar el peor escenario que sería una ICO fraudulenta. [15]

En el factor de las tecnologías empleadas, se encuentran los contratos inteligentes necesarios para culminar el proyecto y brindar seguridad al inversor; no obstante, se pueden presentar errores en la creación de los protocolos y termina siendo perjudicial para una de las partes, asimismo, debe examinarse si se tratará de una Cold Wallet o billetera de escritorio que no se encuentra en línea y es una de las más seguras; pero, en el caso de perder las credenciales de acceso es una pérdida total de su contenido, sin posibilidad de recuperarse; las Hot Wallet son monederos que se encuentran en línea y son administrados por una organización que presta el servicio, es conocido por su capacidad de soporte más sin embargo, el hecho de estar conectados a internet en todo momento trae consigo el riesgo de ser vulnerada su seguridad. [15]

Plataforma de negocios con criptomonedas a través de Blockchain

Actualmente existen varias plataformas que utilizan Blockchain y que ofrecen diferentes servicios y que se consolidan los pagos utilizando criptomonedas, entre ellas tenemos:

La plataforma “CCSCEX | CARACAS COMMODITY EXCHANGE, este ecosistema se basa en tecnologías emergentes como la Blockchain, el crowdfunding y la tokenización, lo que permite mejorar la accesibilidad, la liquidez de los activos y ofrecer oportunidades de inversión atractivas.” [16]

“Rootstock cada Smart Contract desarrollado en Rootstock también puede ser desplegado en Ethereum con total compatibilidad” [17]

“TrustForWills actúa de forma similar a un testamento convencional, pero con la particularidad de que lo hace sobre los perfiles y el patrimonio digitales acumulado a lo largo de la vida de las personas. Mediante contratos inteligentes (smart contracts), la solución permite

facilitar el cumplimiento de las voluntades (wills) de los usuarios de servicios digitales." [18]

Implementación de proyectos basados en Blockchain, para fortalecer la lucha anticorrupción a nivel Colombia como: en Colombia Compra Eficiente y la alcaldía de Medellín en el proceso de licitaciones públicas; la Superintendencia Financiera de Colombia a través de su iniciativa de Sandbox regulatorio ha definido las reglas para el desarrollo de pilotos para la habilitación de intercambio legal de criptoactivos, para viabilizar sus implementaciones asociadas a la tecnología Blockchain; la Procuraduría General de la Nación en conjunto con la Universidad Nacional de Colombia para la vigilancia del PAE (Plan de Alimentación Escolar). [19]

Como se puede observar en los hallazgos encontrados acerca del uso de los contratos inteligentes, cabe destacar que todos los proyectos inHOUSE con Caracas Commodity Exchange presentados, tienen tasas estimadas de retorno de 25% a 50% anual y la compañía Rootstock se encuentra en el rango del rating global de criptomonedas con un volumen de trading diario medio de $531K. Actualmente, su precio es de 24.205.00 USD veinticuatro mil doscientos cinco dólares americanos por cada 1 RBTC (Precio de RSK Smart Bitcoin). [20] [21]

Y en el caso de Colombia cualquier solución de Blockchain diseñada e implementada para una red comercial de cadena de suministro, debe considerar los requisitos de los informes financieros de los participantes, los controles internos y sus partes interesadas, en otras palabras, tener un control riguroso sobre novedades financieras y fiscales con lo cual dar confianza a los usuarios. [20]

MÉTODO O METODOLOGÍA

La metodología de investigación aplicada en este proyecto es documental, enfocada a analizar información emitida por investigadores, empresarios y expertos que emiten juicios en sitios web, sobre Blockchain, donde se contemplaron las siguientes fases:

Fase 1: revisión bibliográfica donde se analizaron resultados de artículos de investigación, libros y repositorios

Fase 2: análisis de conceptos, opiniones o experiencias oportunas a la conversación.

Fase 3: Identificación de plataformas y repositorios, para extraer información documental avalados por estudios técnicos y científicos avalados por instituciones de educación superior.

Fase 4: emisión de juicios y conclusiones

CONCLUSIÓN

Blockchain generalmente se conoce como cadena de bloques, donde se fusionan varias tecnologías cuyo objetivo principal es brindar servicios financieros a las organizaciones, presentando como ventajas la seguridad, transparencia, descentralización y confianza, convirtiéndose en una tecnología novedosa lo que se ha calificado como economía colaborativa, estableciéndose como un elemento que genera aportes innovadores del proceso, lo que genera buenas percepciones sobre el servicio como acciones digitales seguras, ya que en relación con criptoactivos se considera como una buena opción a implementar.

Los contratos inteligentes (Smart Contract), han tomado gran importancia ya que a través de esta herramienta se consolidan negocios y servicios ofertados por varias empresas que emergen en estas tecnologías disruptivas, permitiendo que las criptomonedas a pesar de no tener una validación por el estado, se conviertan en el medio para realizar los pagos de estos convenios.

REFERENCIAS

[1] Banco de la República. “Q16-584 concepto de la secretaría de la junta directiva”. https://www.banrep.gov.co/es/node/40998

[2] S. de prensa. “presidente Nayib Bukele logra atraer proyectos de inversión y se convierte en referencia internacional”. *Presidencia de la república de El Salvador.* Disponible en: https://www.presidencia.gob.sv/presidente-nayib-bukele-logra-atraer-proyectos-de-inversion-y-se-convierte-en-referencia-internacional/

[3] S. de prensa, «presidente Nayib Bukele presenta avances de bitcoin city: el futuro de el salvador», *Presidencia de la república de El Salvador*. Disponible en: https://www.presidencia.gob.sv/presidente-nayib-bukele-presenta-avances-de-bitcoin-city-el-futuro-de-el-salvador/

[4] Bitso. “Support,” centro de ayuda. https://support.bitso.com/hc/es-co/articles/4414905206292-colombia-alianza-bdb-nvio-colombia-

[5] D. Arroyo, J. Díaz, L. Hernández. (2019). ¿Qué sabemos de? Blockchain. (csic ed.) 2019. [en línea] Disponible: https://www.catarata.org/libro/blockchain_94238/

[6] A. Varón y M. Carvajalino “Técnicas para desarrollar aplicaciones web a través de Blockchain”, RITI, vol. 10, n.º 20, pp. 119–129. [En línea]. Disponible: https://doi.org/10.36825/riti.10.20.010

[7] A. Preukschat, *Blockchain: la revolución industrial de internet.* Barcelona, España. Edición gestión, 2017.

[8] R. Viladot & C. González. (2020). *Criptomonedas para dummies.* Barcelona, España. CEAC, 2020.

[9] National Institute of Standards and Technology Gaithersburg. digital signature standard (dss). nvlpubs. https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.186-4.pdf

[10] J. Torres (2019). *Criptomonedas: qué son, cómo utilizarlas y por qué van a cambiar el mundo.* España. Editorial Planeta, 2019.

[11] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, F. Wang (2019). “Blockchain-enabled smart contracts: architecture, applications, and future trends”. ieee transactions on systems, man, and cybernetics: systems, vol. 49, no. 11, pp. 2266-2277. https://doi.org/10.1109/tsmc.2019.2895123

[12] M. Bal, y C. Ner “NFTracer: a non-fungible token tracking proof-of-concept using hyperledger fabric”, arxiv.org, 2019. https://doi.org/10.48550/arXiv.1905.04795

[13] Q. Wang, R. Li, Q. Wang, y S. Chen “Non-fungible token (nft): overview, evaluation, opportunities and challenges”, arxiv.org, 2021. https://doi.org/10.48550/arXiv.2105.07447

[14] D. Echavarría “Surgimiento de las icos: implicaciones para el caso colombiano”. *Revista de derecho*

privado. 2019 vol. 38 pp. 143–172. https://doi.org/10.18601/01234366.n38.06

[15] B. Fonticiella. *"La protección del inversor minorista en el panorama fintech.* ESPAÑA. Editorial Dykinson, s.l. 2022.

[16] Ecosistema ccscex "¿por qué caracas commodity exchange?". https://ecosistema.ccscex.com/ecosistema-ccscex/whitepaper/por-que-caracas-commodity-exchange

[17] Rootstock "Construyamos juntos sobre Bitcoin". https://rootstock.io/

[18] AtSistemas, "atSistemas desarrolla una solución blockchain que actúa como testamento para el patrimonio digital de los usuarios". https://www.atsistemas.com/es/novedades/noticias/trustforwills

[19] MinTIC. "Guía de referencia para la adopción e implementación de proyectos con tecnología blockchain para el estado colombiano". 2021. https://gobiernodigital.mintic.gov.co/692/articles-179085_recurso_3.pdf

[20] Criptoinforme. "¿qué es caracas commodity exchange (ccscex) y qué puede ofrecer?", [en línea]. disponible: https://criptoinforme.com/comunicado-de-prensa/que-es-caracas-commodity-exchange-ccscex-y-que-puede-ofrecer/

[21] Beincripto. "rootstock rsk (rbtc). información de precios, capitalización de mercado, gráficos y fundamentos – beincrypto", recuperado: 23 de julio de 2020. https://es.beincrypto.com/precio/rootstock/