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

CRIPTOMONEDA IOTA UTILIZANDO TECNOLOGÍA TANGLE, UNA ALTERNATIVA A BLOCKCHAIN

Jefferson Raúl Santos Ramírez
Asesorado por el Ing. Mario José Bautista Fuentes

Guatemala, enero de 2020

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

CRIPTOMONEDA IOTA UTILIZANDO TECNOLOGÍA TANGLE, UNA ALTERNATIVA A BLOCKCHAIN

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

JEFFERSON RAÚL SANTOS RAMÍREZ
ASESORADO POR EL ING. MARIO JOSÉ BAUTISTA FUENTES

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN CIENCIAS Y SISTEMAS

GUATEMALA, ENERO DE 2020

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

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

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Inga. Aurelia Anabela Cordova Estrada
EXAMINADOR	Ing. Luis Fernando Espino Barrios
EXAMINADOR	Ing. Sergio Arnoldo Méndez Aguilar
EXAMINADOR	Ing. William Estuardo Escobar Argueta
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

HONORABLE TRIBUNAL EXAMINADOR

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

CRIPTOMONEDA IOTA UTILIZANDO TECNOLOGÍA TANGLE, UNA ALTERNATIVA A BLOCKCHAIN

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería en Ciencias y Sistemas, con fecha 25 de septiembre de 2019.

Jefferson Raúl Santos Ramírez

Guatemala, 11 de noviembre de 2019

Ing. Carlos Gustavo Alonzo
Director de Escuela
Escuela de Ingeniería en Ciencias y Sistemas
Facultad de Ingeniería
Universidad de San Carlos de Guatemala

Por este medio hago constar que el estudiante universitario Jefferson Raúl Santos Ramírez que se identifica con CUI No. 1739828750101 y código estudiantil No. 200819003 ha concluido satisfactoriamente el trabajo de graduación que lleva por título "CRIPTOMONEDA IOTA UTILIZANDO TECNOLOGÍA TANGLE, UNA ALTERNATIVA A BLOCKCHAIN" bajo mi asesoría donde apruebo el contenido del mismo.

Para su conocimiento y efectos, sin otro particular, me suscribo.

Mario Jose Bautista Fuentes
Ing. En C.C Y Sist...
Colegiado. 10017

Vo. Bo. _____

Ing. Mario José Bautista Fuentes
Col. 10017
Asesor

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

Guatemala, 15 de noviembre de 2019

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

Respetable Ingeniero Alonzo:

Por este medio hago de su conocimiento que he revisado el trabajo de graduación del estudiante **JEFFERSON RAÚL SANTOS RAMÍREZ** con carné **200819003 y CUI 1739 82875 0101** titulado **"CRIPTOMONEDA IOTA UTILIZANDO TECNOLOGÍA TANGLE, UNA ALTERNATIVA A BLOCKCHAIN"** y a mi criterio el mismo cumple con los objetivos propuestos para su desarrollo, según el protocolo aprobado.

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

Atentamente,

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

ESCUELA DE INGENIERÍA EN CIENCIAS Y SISTEMAS

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÌA
ESCUELA DE INGENIERÍA EN
CIENCIAS Y SISTEMAS
TEL: 24188000 Ext. 1534

El Director de la Escuela de Ingeniería en Ciencias y Sistemas de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer el dictamen del asesor con el visto bueno del revisor y del Licenciado en Letras, del trabajo de graduación, ***"CRIPTOMONEDA IOTA UTILIZANDO TECNOLOGÍA TANGLE, UNA ALTERNATIVA A BLOCKCHAIN"*** *realizado por el estudiante, JEFFERSON RAÚL SANTOS RAMÍREZ, aprueba el presente trabajo y solicita la autorización del mismo.*

"ID Y ENSEÑAD A TODOS"

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION DE INGENIERIA EN CIENCIAS Y SISTEMAS

MSc. Ing. Carlos Gustavo Alonzo
Director
Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, 28 de enero de 2019

Universidad de San Carlos
de Guatemala

Facultad de Ingeniería
Decanato

DTG. 031.2020

La Decana de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería en Ciencias y Sistemas, al Trabajo de Graduación titulado: **CRIPTOMONEDA IOTA UTILIZANDO TECNOLOGÍA TANGLE, UNA ALTERNATIVA A BLOCKCHAIN,** presentado por el estudiante universitario: **Jefferson Raúl Santos Ramírez,** y después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, autoriza la impresión del mismo.

IMPRÍMASE:

Inga. Anabela Cordova Estrada
Decana

Guatemala, enero de 2020

/gdech

ACTO QUE DEDICO A:

Mi madre	Por ayudarme a conseguir mis metas y objetivos, estar siempre en las buenas y en las malas, por todo el esfuerzo en brindarme las condiciones necesarias para estudiar y por todo su amor incondicional.
Mi padre	Por formarme con valores, amor, por ser él una importante influencia en mi carrera y apoyo en todo momento.

AGRADECIMIENTOS A:

Universidad de San Carlos de Guatemala	Por permitirme acceder a la educación superior y enseñarme a estar orgulloso de esta casa de estudios.
Facultad de Ingeniería	Por brindarme el conocimiento y los conceptos necesarios para mi carrera profesional.
Mis amigos de la facultad	Diego Fuentes, Eliseo Sahuay, Josué Salvador, por apoyarme en la culminación de mi carrera.
Ing. Mario José Bautista Fuentes	Por compartir sus conocimientos en los cursos de la carrera, por el apoyo y asesoría en la elaboración de la tesis.
Germey Alonzo	Por apoyarme y ayudarme en el inicio de mi carrera y siempre estar pendiente de mis avances.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

LISTA DE SÍMBOLOS

Símbolo	Significado
BTC	Bitcoin
$	Dólar estadounidense
%	Porcentaje
Q	Quetzal

GLOSARIO

Altcoin	Moneda digital alternativa a Bitcoin.
Amazon	Organización de nacionalidad estadounidense encargada del comercio electrónico y servicios de *cloud computing*.
API	Conjunto de comandos y funciones informáticas que permiten a los desarrolladores crear programas específicos.
Binance	Plataforma para intercambiar criptomonedas.
Bitcoin	Moneda digital descentralizada.
Blockchain	Red distribuida basada en criptografía en la cual la información se almacena en un conjunto de bloques entrelazados entre sí.
Broker	Intermediario entre compradores y vendedores en el mercado de valores.
Consenso	Se basa en que todos los miembros de una criptomoneda deben estar de acuerdo con la validación de los bloques y su contenido.

Criptografía	Arte de escribir con clave secreta o de un modo enigmático.
Criptomoneda	Moneda basada exclusivamente en la criptografía.
Cuántico	Se refiere a lo vinculado con unos ciertos saltos de la energía al emitir o absorber radiación.
DAG	Es una red en el que cada nodo representa una variable y cada arco una dependencia probabilística, en la cual se especifica la probabilidad condicional de cada variable dados sus padres.
DDoS	Una ocasión en que una red de computadoras o un sitio web intencionalmente no funciona correctamente, por un gran número de usuarios que envían datos al mismo tiempo.
DLT	Es una red descentralizada que no necesita una base de datos central ni una entidad central de toma de decisión.
Ether	Criptomoneda de la red Ethereum.
Ethereum	Una red de código abierto basada en la tecnología Blockchain cuya propuesta es el desarrollo de aplicaciones descentralizadas con intención de evitar la censura, los intentos de fraude o la interferencia de una tercera parte en las mismas.

Exchange	Casa de cambio digital que permite cambiar dinero fiduciario por criptomonedas o criptomonedas entre sí.
Hash	Es un código de salida que se obtiene a partir de aplicar un algoritmo sobre una cadena de entrada lo que permite saber si dicha cadena original ha sido alterada.
Hashrate	Es la velocidad con la que un procesador genera valores *hash* en un periodo de tiempo.
IoT	Es un sistema de dispositivos de computación interrelacionados u objetos que tienen identificadores únicos y la capacidad de transferir datos a través de una red, sin requerir de interacciones humano a humano o humano a computadora.
IOTA	Criptomoneda que fue producida especialmente para internet de las cosas, basaba en Tangle.
Minería	Combinación de recursos de varios mineros para obtener una potencia de minado mayor y así conseguir mayores recompensas por la apertura de bloques.
Peer-to-peer	Hace referencia a redes descentralizadas donde se comparte información entre dos usuarios mediante

	conexión a la red sin más intermediario que un software que los conecta.
PoW	Es un sistema de validación de las transacciones de una red mediante la resolución de operaciones matemáticas a través de equipos informáticos especializados.
Tangle	Libro contable distribuido donde se tienen nodos conectados en bloques. Cada nodo actúa como un minero. No hay comisiones de transacciones ni mineros.
Wallet	Es el software que permite almacenar y transaccionar las criptomonedas sin permiso ni mediación de nadie.

RESUMEN

A diario, surgen nuevas criptomonedas en las cuales se puede invertir esperando crecimiento y uso; la mayoría toma cierta tendencia a desarrollar bajo el concepto de Blockchain, por ejemplo, Bitcoin, Ethereum. IOTA tiene como objetivo facilitar los pagos y las comunicaciones entre los dispositivos que forman parte del internet de las cosas; un tema que se ha convertido tendencia en internet.

Actualmente, en la web se tienen problemas de ataques DDoS o ataques cibernéticos; estos vienen a perjudicar en el tema de seguridad o en la extracción de bitcoins. Al igual que lo hará la computación cuántica cuando se establezca en el futuro, esto es un problema para el sistema Blockchain; con IOTA se mitigan estos riesgos ya que IOTA trabaja con el sistema Tangle que tiene una resistencia a la computación cuántica.

Se ha desarrollado un marco de trabajo teórico orientado hacia la criptomoneda IOTA y la tecnología Tangle, así como distintos temas de seguridad de datos, un tema crítico para las empresas y las personas.

OBJETIVOS

General

Presentar una comparación de dos tecnologías que desarrollan criptomonedas con inclinación a favor de IOTA debido a la utilización de nuevas técnicas con visión al futuro del procesamiento de la computación.

Específicos

1. Explicar por qué la tecnología Tangle tendrá resistencia cuántica y por qué Blockchain no puede cubrir la computación cuántica.

2. Facilitar la búsqueda de información sobre las tecnologías Blockchain y Tangle acerca de las características, el rendimiento, la seguridad, los algoritmos, entre otros.

3. Mostrar los diferentes usos que puede tener IOTA en el mundo de la computación y tecnología.

4. Motivar a las personas a la inversión en IOTA debido al bajo precio que se encuentra en el mercado con potencial de aumentar su valor en los próximos años debido a su apuesta por una tecnología distinta a Blockchain.

INTRODUCCIÓN

Internet se ha convertido hoy en día en una herramienta muy utilizada para realizar transacciones, negocios y operaciones; actualmente existe otro tema que está tratándose internacionalmente, el internet de las cosas. La gran adversidad que tiene el uso de internet y que genera una preocupación en las personas es la seguridad de los datos. Blockchain es una solución que provee seguridad, pero en el futuro tendrá problemas con la computación cuántica.

La investigación desarrollará los temas de seguridad, criptografía, Blockchain, resistencia cuántica, algoritmos cuánticos, minería de datos, sistema Tangle, escalabilidad, internet de las cosas; además en qué otras áreas se puede desarrollar IOTA. También, el tema de inversión en la bolsa de valores para realizar comparaciones.

Se utilizará el auge de las criptomonedas y el desconocimiento sobre IOTA para generar una investigación donde los lectores de la tesis puedan encontrar información moderna y sobre contenidos futuros; de esa forma podrá comparar y evaluar las tendencias de las criptomonedas en el futuro para realizar una inversión con base en la información presentada.

Esta investigación pretende dar a conocer en la universidad y en el país otra alternativa a Blockchain, que es una herramienta muy popular mundialmente; para conocer otras opciones en donde se pueden realizar inversiones y aprender nuevas tecnologías.

1. CRIPTOMONEDAS

1.1. Definición

Una criptomoneda es una moneda electrónica que se puede aplicar para transferir dinero de forma digital a otra persona de forma segura, sin tener que usar intermediarios, por ejemplo, una institución financiera o Visa. Esto ahorra en costos al inversionista, eximiéndolo de pagar comisión. Las criptomonedas trabajan con el sistema Blockchain, una tecnología bastante confiable. La criptomoneda más famosa es Bitcoin (BTC). Bitcoin es una moneda electrónica global y descentralizada.

La mayoría de los sistemas de pago se realizan en una red centralizada. El problema de esta modalidad es incurrir en costos de transacción innecesarios y excesivos. Por lo general, esto lo realiza un servidor central que realiza un seguimiento de los saldos; es decir, la tarjeta de crédito y los bancos. También, puede tomar varios días para que un banco se comunique con otra institución, por lo que enviar dinero se vuelve costoso y toma demasiado tiempo.

Un sistema descentralizado significa que la red está desarrollada por sus usuarios donde ningún tercero puede controlar. Ni los bancos centrales ni los gobiernos de cualquier país tienen poder en este sistema.

Las criptomonedas pueden ser alternativa de inversión. El comercio de criptomonedas es un mercado en crecimiento conforme pasan los años, ahora se ofrecen opciones de cobertura y flexibilidad, similarmente al mercado de

valores tradicional. Mientras el mercado criptográfico progresa, las opciones de cobertura prosperan.

Obtener ganancias en los mercados bursátiles tradicionales puede ser complejo y toma un tiempo considerable; comenzar con operaciones regulares requiere información personal sustancial, a veces, depósitos más grandes. Los corredores de bolsa son necesarios solo para realizar una operación inicial. Además, los márgenes de beneficio entre las acciones regulares y el mercado de cifrado son significativamente diferentes. Las criptomonedas son altamente volátiles en comparación con el mercado de valores tradicional, producen grandes fluctuaciones en el valor de los activos, generando potencial para generar mayores ganancias.

En la actualidad, el mercado de criptomonedas todavía está relativamente desregulado, por lo tanto, es más fácil comenzar a comerciar con criptomonedas. Se requiere menos capital para generar ganancias potenciales, los procesos involucrados para registrarse son mucho menos restrictivos, más fáciles y no se requieren intermediarios. Las criptomonedas se pueden comercializar desde casi cualquier lugar del mundo, siempre que se disponga de una conexión a internet, haciendo que la criptomoneda sea una de las opciones de inversión más flexibles en el presente.

.

1.2. Historia y origen

Todo comenzó en la década de 1980 por un criptógrafo estadounidense llamado David Chaum. Inventó la primera forma de generar dinero en internet llamada DigiCash. Terminó en bancarrota en 1998. Varias empresas surgieron para hacer algo nuevo en el mundo de la moneda digital, pero fracasaron debido a su base en la centralización.

Otro proyecto llamado e-Gold se introdujo en el mundo que aceptó el oro de los usuarios a cambio de unidades digitales de e-Gold en monedas denominadas onzas de oro. Dejaron de tener actividad debido a sus dudosas actividades ilegales.

El mundo tenía la necesidad de tener algo de poder confiable y descentralizado. En 2008, una nueva criptomoneda llamada Bitcoin se mencionó por primera vez en un documento técnico titulado ‘Bitcoin, un sistema de efectivo electrónico de igual a igual’, escrito por Satoshi Nakamoto. Solo hay un nombre asignado a la invención de Bitcoin; nadie sabe quién es Satoshi Nakamoto, si es una sola persona o un grupo de personas, continúa siendo un misterio.

Se desarrolló sobre los conceptos de descentralización, anonimato y Blockchain. A principios de 2009, se lanzó el primer Bitcoin; posteriormente, los entusiastas de la tecnología comenzaron a intercambiar y extraer bitcoins. Su valor en la fase inicial fue casi nulo. Esto se debe a que nunca se comercializó y solo se dedicaron a minar bitcoins. Como era una moneda descentralizada, nadie sabía su valor monetario.

La primera transacción registrada de Bitcoin a cambio de dólares estadounidenses fue cuando una persona llamada Martti envió 5 050 bitcoins a una organización llamada NewLiberty Standard por $ 5,02. Esta transacción hizo a la gente pensar acerca del valor real de Bitcoin.

Antes de esto, nadie había vendido ni comprado bitcoins, por lo que NewLiberty Standard ideó su propio método para determinar el valor de Bitcoin. El valor de Bitcoin se determinó calculando el costo de la electricidad necesaria

para generar la moneda, a partir de su propia factura de electricidad. El resultado fue $ 1 por 1 000 bitcoins.

El 22 de mayo de 2010, Laszlo Hanyecz compró dos pizzas por un valor de $ 41 al entregar 10 000 BTC a cambio. Este día ahora se celebra como el 'Día de la pizza Bitcoin'. Así, la gente comenzó a familiarizarse con Bitcoin y su valor se disparó en la bolsa de valores. El valor de Bitcoin ha tenido muchos altibajos durante su historia. El precio de Bitcoin consiguió llegar alrededor de $1 000 a fines de 2013. La tasa más alta alcanzada hasta ahora es de aproximadamente $ 20 000. Ahora, fluctúa alrededor de $ 10 000.

Con la creciente popularidad de Bitcoin, se lanzaron muchas otras criptomonedas en el mercado que también se conocen como Altcoins, colectivamente. Actualmente, existen más de 1 000 criptomonedas en circulación, por ejemplo, una de los más populares es Ethereum.

1.3. Criptografía

La palabra *cripto* es de origen griego y significa escondido, en este contexto, anónimo. Dependiendo de la configuración, la tecnología de criptografía implementada asegura el anonimato completo o seudo. La criptografía respalda la seguridad de las transacciones y los usuarios, la independencia de los procedimientos de una autoridad central y la defensa contra el doble gasto.

La tecnología de criptografía se utiliza para diversos propósitos: asegurar las múltiples transacciones que ocurren en la red; examinar la generación de nuevas unidades monetarias; revisar la transferencia de activos digitales y *tokens*.

Para simplificar, la criptografía es una tecnología para enviar mensajes seguros entre dos o más elementos: el remitente cifra un mensaje utilizando un tipo de clave y un algoritmo, envía esta forma cifrada de mensaje al receptor; entonces, el receptor lo descifra para ver el mensaje original.

La clave de cifrado es la característica más importante de la criptografía. Hace que un mensaje, una operación o un valor de datos sea ilegible para un lector o receptor no autorizado, solo el destinatario puede leerlo y transaccionarlo. La clave elabora que la información sea criptográfica o anónima.

Algunas de las herramientas que se desplegaron para la criptografía tradicional tienen otras funciones útiles. Las dos más relevantes son el *hash* y las firmas digitales. Por ello, aunque ninguna de estas herramientas implique el envío de mensajes secretos, todavía se consideran formas de criptografía.

El *hash* es usado por las criptomonedas para verificar de manera óptima la integridad de los datos. Es un procedimiento para tomar grandes cantidades de datos y representarlos sistemáticamente como un número corto que es complejo de replicar.

El *hash* se utiliza en gran medida para conservar la estructura de los datos de Blockchain, que contiene los saldos de las cuentas de los usuarios. Además, se utiliza para codificar las direcciones de las cuentas de las personas y como parte del proceso de codificación de operaciones entre cuentas.

Finalmente, el *hash* se usa para generar acertijos matemáticos que hacen posible la minería de bloques, una característica importante en muchas

criptomonedas. El *hashing* hace un uso intensivo de los cifrados de bloque, una tecnología que se utilizó originalmente para la criptografía tradicional.

Las firmas digitales le permiten a una persona tomar un poco de información oculta que posee y demostrar que tiene esa información, sin divulgarla. Las criptomonedas permiten a los usuarios certificar transacciones monetarias con estas firmas digitales para evidenciar a la red que el propietario de una cuenta con dinero acordó una transacción para gastar ese dinero.

1.4. Conceptos clave

Algunos conceptos importantes que se deben mencionar de las criptomonedas son:

1.4.1. Minería

Es el proceso de validar las transacciones de otras personas con una computadora y luego agregarlas a la larga lista pública de todas las transacciones conocidas como Blockchain. A cambio, las personas son recompensadas con criptomonedas.

Cada vez que se realiza una transacción, un minero de criptomonedas es responsable de garantizar la autenticidad de la información y actualizar la cadena de bloques con la transacción. El proceso de minería implica competir con otros mineros para resolver problemas matemáticos complicados con funciones *hash* criptográficas que están asociadas con un bloque que contiene los datos de la transacción.

El primer minero de criptomonedas que descifra el código es recompensado al autorizar la transacción, a cambio del servicio prestado, los mineros obtienen pequeñas cantidades de criptomonedas. Sin embargo, para ser competitivo, se necesita una computadora con *hardware* especializado.

1.4.2. Billeteras de criptomonedas

Es básicamente un programa informático que permite recibir, enviar y controlar el saldo de las criptomonedas. La billetera consiste en tener dos claves: una clave pública y una clave privada. La clave pública es la dirección de una billetera. Esta información es lo que otras personas usan para enviar monedas. La clave privada es lo que permite enviar monedas a diferentes destinatarios.

1.4.3. Transparencia

Cada transacción de criptomonedas se registra en libro mayor digital. Los datos que contiene este libro digital son de acceso público para todas las computadoras de una red. Esto quiere decir que cualquiera puede ver todas las transacciones y la cantidad de monedas que posee cada dirección de criptomonedas. A pesar de esta característica, las direcciones no se pueden usar para identificar al dueño de las monedas.

1.4.4. Moneda digital

Es una forma de moneda que está disponible solo en forma digital o electrónica, no está disponible de manera física. También, se llama dinero digital, dinero electrónico, moneda electrónica o dinero en efectivo cibernético.

Las monedas digitales son intangibles y solo pueden ser transaccionar mediante el uso de computadoras o billeteras electrónicas que están conectadas a internet. Las monedas digitales ofrecen numerosas ventajas.

Los pagos en monedas digitales se realizan directamente entre las partes que realizan las transacciones sin la necesidad de intermediarios, las transacciones suelen ser instantáneas y de bajo costo. Esto es mejor en comparación con los métodos de pago tradicionales que involucran instituciones financieras. Las transacciones electrónicas digitales basadas en divisas también aportan el mantenimiento de registros y la transparencia necesarios en las operaciones.

1.4.5. Satoshi

Es la unidad más pequeña de la criptomoneda Bitcoin. Lleva el nombre de Satoshi Nakamoto, el creador del protocolo utilizado en Blockchain y la criptomoneda Bitcoin. La relación satoshi a Bitcoin es de 100 millones de satoshis a un Bitcoin.

Una criptomoneda se puede dividir en unidades más pequeñas, al igual que la libra se divide en libras y el dólar en centavos. En el tema de bitcoins, la unidad más pequeña disponible se llama satoshi.

1.4.6. *Exchanges*

Es cualquier sistema que opera sobre la base del comercio de criptomonedas con otros activos. La operación principal del *exchange* es permitir la compra y venta de activos digitales. Puede ser un creador de

mercado que generalmente toma los diferenciales de oferta y demanda como una comisión de transacción por su servicio cobrando tarifas.

2. DEFINICIÓN IOTA

2.1. ¿Qué es IOTA?

IOTA es un protocolo contable distribuido escalable, descentralizado, sin costo, modular, de código abierto, que utiliza la tecnología llamada Tangle. Deriva su nombre de la abreviatura de internet de las cosas. Algunas características que tiene IOTA son:

- Escalable: permite una gran cantidad de transacciones por segundo y no tiene límite.
- Descentralizado: no hay servidor central ni propietario.
- Sin tarifa: las transacciones no tienen tarifa de red.
- Modular: otras tecnologías pueden conectarse a IOTA.
- Código abierto: el código del programa se puede descargar en línea.

IOTA se enfoca inicialmente en servir como eje central del emergente internet de las cosas, al permitir la comunicación máquina a máquina, micro y nano pagos, así como otros casos de uso.

IOTA se estableció como una derivación muy vinculada a la tecnología Blockchain, pero es mucho más avanzada debido a que utiliza diferentes sistemas y ya es distinguida en la prensa de innovación como Forbes, Huffington Post, entre otros. Varias universidades ya reconocieron la capacidad de esta criptomoneda y decidieron trabajar con IOTA.

Fue fundada en 2014 para ofrecer una red fácilmente implementable para internet de las cosas. Ofrece una gran escalabilidad, resistencia cuántica y descentralización para los diferentes casos de uso de internet de las cosas e interacción humana.

2.2. Historia de IOTA

Los fundadores de IOTA, David Sønstebø, Sergey Ivancheglo, Serguei Popov y Dominik Schiener habían estado trabajando con Blockchain desde 2010 a 2011. IOTA nace de un *startup* de hardware, que estaba trabajando en un nuevo microprocesador ternario bajo el título de 'Jinn'. Un procesador ternario se compone en tres estados en lugar de dos, como lo hacen casi todos los procesadores binarios modernos. Una de las principales diferencias de esta historia de origen frente a otros proyectos es que IOTA surgió de una necesidad real. No fue el impulso de crear una nueva y sofisticada tecnología de gráfico acíclico dirigido (DAG) lo que inició el proyecto, sino el aparente problema de la solución transaccional para internet de las cosas y la falta de soluciones existentes en la actualidad.

Empezaron creando el Blockchain 2.0, fue la primera prueba completa de Blockchain, tenía características como un intercambio descentralizado de activos, registro de nombres y muchos más. Después, se dieron cuenta que tenían que comenzar desde cero para satisfacer las exigentes demandas del internet de las cosas. Con eso en mente, nació el Tangle a mediados de 2015. Serguei Popov, doctor en matemáticas, creó la base técnica necesaria para el Tangle, que había sido programado por Sergey Ivancheglo y Dominik Schiener.

IOTA organizó una convención en diciembre de 2015 en la que se vendió todo el *token* de IOTA a los participantes. IOTA recolectó 1 337 bitcoin para su

proyecto. Esto significa que estos *tokens* estaban minados previamente, no se realizó ninguna extracción adicional. Otra parte importante del *token* fue donada a la fundación IOTA. Fue fundada en Berlín, Alemania, esta fundación ayuda a desarrollar IOTA.

Con este modelo, IOTA también puede obtener ayuda pública, ya que el proyecto no está orientado a las ganancias. Se unió la empresa Bosch para trabajar en conjunto. El sistema sigue creciendo y la fase beta pública comenzó en 2016. Otras compañías y corporaciones se unieron para probar IOTA, como Volkswagen e Innogy, así como otras.

2.3. ¿Cómo funciona IOTA?

El primer paso de IOTA fue encontrar y habilitar un nuevo concepto alternativo en lugar de otro Blockchain. Dado que Blockchain es la razón por la cual Bitcoin está atascado en siete transacciones por segundo, no podría haber nada parecido a Blockchain. El resultado fue una base de datos distribuida de la tercera generación: el Tangle. No es un sistema nuevo, pero no es Blockchain.

Resuelve el problema de escalabilidad con un nuevo enfoque, en el que no se escriben bloques y los datos se procesan en paralelo. Del mismo modo, las nuevas transacciones son confirmadas por varios participantes y no solo por los mineros, como lo hacen en las otras criptomonedas. Estos son los pasos para una nueva transacción:

- Un dispositivo tiene que confirmar dos transacciones anteriores, esto se hace automáticamente por el programa informático.

- Después de verificar y validar estas transacciones, se envían en la red.

- Esta autenticación se confirma con un identificador único, que es un número utilizado una vez.

Esa es una manera de evitar que personas que cometen delitos cibernéticos congestionen la red. IOTA resolvió bien el problema fundamental de las aplicaciones modernas de Blockchain con una escalabilidad óptima.

2.4. ¿Qué problema resuelve IOTA?

El problema resuelto por IOTA es el tema del internet de las cosas. Los fundadores de IOTA tuvieron la visión de que IOTA se convertiría en el eje central del internet de las cosas. Esto significa que los dispositivos inteligentes utilizarían IOTA como plataforma, por ejemplo, un refrigerador inteligente podría descubrir que un producto está descompuesto.

Para comunicar esto, el refrigerador puede usar sus sensores para comunicarse en IOTA, de modo que su aplicación móvil muestre una notificación.

Otro ejemplo es la administración automática de la luz, para la cual hoy en día muchos usan los dispositivos domésticos inteligentes caros e ineficientes. Con IOTA pueden acceder a la misma plataforma y comunicarse entre ellos sin problemas.

Haciendo una comparación de lo que puede resolver el internet de las cosas, se tiene la siguiente tabla:

Tabla I. **Comparación internet y el internet de las cosas**

Tema	Internet tradicional y normal	Internet de las cosas
Creación de contenido.	Humanos.	Máquinas.
Combinación del contenido.	Bajo demanda.	Al ingresar información e inducir acciones como resultado.
Valor.	Respondiendo demandas.	Respondiendo estados críticos.
Estado.	El contenido se distribuye aleatoriamente en línea y puede ser clasificado por motores de búsqueda.	Principalmente datos.

Fuente: elaboración propia.

Las aplicaciones basadas en Blockchain no podrán manejar la gran cantidad de datos provenientes de la multitud de sensores. Es necesario un sistema que procese una gran cantidad de transacciones de manera transparente y rápida, sin un cuello de botella. IOTA ha abordado estos problemas y quiere resolver los siguientes temas:

- Lograr escalabilidad y descentralización
- Habilitar la comunicación de máquina a máquina
- Realizar una prueba de trabajo para confirmar transacciones

2.5. Características

Las principales características de IOTA son:

2.5.1. Escalabilidad

IOTA no utiliza bloques, por lo tanto, se agregan una a una las transacciones a la red, haciendo que se tenga una mejor escalabilidad y una menor latencia. Para publicar una transacción, se deben validar dos transacciones previamente, mientras más transacciones se vayan validando, el Tangle será óptimo y más seguro, debido a que irá certificando las transacciones una por una.

2.5.2. Tarifas de transacción

Se pueden transmitir tanto valor como datos sin pagar ninguna comisión. No se tiene que pagar ninguna tarifa de transacción a medida que IOTA logra un consenso sobre la validez de las transacciones sin la participación de ningún minero. IOTA es el primer protocolo de liquidación transaccional que admite realizar transacciones u operaciones incluso por debajo de los valores *peer-to-peer* sin ninguna tarifa de transacción para el remitente o el destinatario. Como tal, IOTA conseguiría ser la columna vertebral de los casos de uso de micropagos y nanopagos actuales y futuros. Sin embargo, las personas aún incurren en costos por la energía para confirmar otras dos transacciones, cuando quieren ejecutar una.

2.5.3. Comunicación en IOTA

Los mensajes en la comunicación se envían de manera autenticada y enmascarada ofreciendo la posibilidad de enviar un flujo de datos cifrados de forma segura a través de Tangle. Los datos están protegidos en el libro mayor y todas las personas autenticadas pueden acceder a los datos.

2.5.4. Modular

IOTA ofrece flexibilidad a todos los elementos de este protocolo, gracias a esta característica las transacciones son más rápidas, se cuenta con un mantenimiento óptimo para los nodos y las personas tendrán la máxima libertad para ajustarse al sistema según sean sus necesidades individuales.

2.5.5. Sin terceros implicados

Como se menciona en la escalabilidad, Tangle no utiliza los bloques como en Blockchain, tampoco lleva un orden definido de los elementos que forman parte del sistema, en virtud de que las transacciones pueden almacenarse en diversos dispositivos utilizando varias ubicaciones mezcladas.

Ya que IOTA no utiliza mineros, una prueba de trabajo valida dos transacciones previas por cada una de las transacciones, el sistema itera todas las transacciones y las va uniendo en direcciones, independientemente del orden. Cuando Tangle finaliza este proceso, las direcciones muestran los resultados o valores y el usuario certifica que los resultados son correctos en las direcciones.

2.5.6. Interoperabilidad

Como varias tecnologías ofrecen ventajas para casos de uso muy especiales, la tecnología Blockchain se ha establecido en algunas industrias. Por lo tanto, IOTA ofrece una API, a través de la cual se pueden conectar otras plataformas criptográficas como Ethereum.

2.6. Desventajas

Algunas desventajas que se pueden mencionar son:

- A diferencia de los sistemas basados en Blockchain como Bitcoin y Ethereum, la dificultad de la prueba de trabajo no es adaptativa en la red IOTA. Esto significa que la seguridad de Tangle depende directamente de cuántas transacciones se están procesando y no hay forma de adaptar el nivel de seguridad a las condiciones del mundo real.

- El objetivo de IOTA de servir como una red de pago de máquina a máquina significa que habrá una alta velocidad de dinero en la red. Esto podría dañar el valor de IOTA como una inversión a largo plazo porque la moneda actuará menos como una reserva de valor.

- El protocolo utiliza un sistema de numeración llamado ternario balanceado, que contiene los 3 dígitos: -1, 0 y 1. IOTA está diseñado para ejecutarse en hardware y redes de comunicación existentes, que utilizan el sistema binario. Esto significa que toda su notación ternaria interna debe estar encapsulada en binario, lo que aumenta el almacenamiento y la sobrecarga computacional.

2.7. MIOTA

El principal producto de IOTA es MIOTA, actualmente la moneda digital del Tangle, una moneda creada para la economía de la máquina que ofrece soluciones con respecto a la tecnología de contabilidad distribuida como Blockchain. Un MIOTA es un millón de IOTA.

El objetivo principal de MIOTA es que la información generada por los dispositivos inteligente sea transmitida de forma segura a un tercero, que logre crear un mercado de datos para que sean compartidos o vendidos.

3. TECNOLOGÍA TANGLE Y PROCEDIMIENTOS DE SEGURIDAD

3.1. Descripción

IOTA se basa en la nueva tecnología Tangle, que tiene como expectativa superar las desventajas sistemáticas de Blockchain. Al igual que con las aplicaciones Blockchain, el Tangle es un libro mayor, es decir, una base de datos distribuida en la que se almacenan todas las transacciones. Todos los usuarios de la red pueden ver las transacciones almacenadas en el libro mayor distribuido (DLT).

Un DLT “es un consenso de datos digitales replicados, compartidos y sincronizados distribuidos geográficamente en múltiples sitios, países o instituciones. No hay administrador central o almacenamiento de datos centralizado”[1].

La innovación importante en IOTA es que el libro mayor se describe a través del Tangle. El Tangle no es una tecnología Blockchain porque se basa en un gráfico acíclico directo (DAG). El Tangle es un tipo especial de gráfico dirigido porque contiene las transacciones. Se representan como nodos.

Tangle busca resolver el inconveniente del consenso en una red de comunicaciones distribuidas entre dispositivos o nodos sin necesidad de servicios centralizados de certificación de transacciones.

[1] *IOTA, conectando el mundo*. https://www.paradigmadigital.com/dev/iota. Consulta: 3 de octubre de 2019.

En IOTA, no hay bloques escritos, pero las transacciones hacen referencia a dos transacciones anteriores. Esto lleva a un consenso, porque un usuario confirma directamente estas dos transacciones e indirectamente confirma las transacciones anteriores de las dos transacciones directamente referenciadas.

Esto confirma que esta subárea del Tangle es válida y cumple con las reglas del protocolo. Por lo tanto, esta red consta de un gran grupo de participantes activos, no hay formación de bloques, como es el caso de Bitcoin, en Tangle los nodos se organizan en grupos. Además, el proceso de consenso en IOTA no está separado de las transacciones, sino que es una parte de él que hace que IOTA sea escalable.

El Tangle se programa bajo el sistema ternario, es una desviación del código binario, que utiliza tres dígitos, los cuales son: -1, 0 y 1, esto equivale a que son 3 estados en total. Toda la computación actual trabaja bajo el sistema binario, pero Tangle se adapta para trabajar bajo los dos sistemas, tanto binario como ternario.

Una transacción en IOTA tiene varios parámetros, los cuales son:

- Peso propio: es un número, potencia de 3, el nodo asigna este número a la transacción, es proporcional al esfuerzo computacional que hizo el nodo al definir el enigma criptográfico. Las transacciones más importantes son las que tienen pesos más altos.

- Peso acumulado: es el peso propio de una transacción más la suma de todos los pesos propios de las transacciones que aceptan a una transacción, tanto directa como indirectamente.

- Puntuación: es la suma del peso propio de una transacción más el total de la suma de los pesos propios de todas las transacciones que la transacción ha aprobado directa o indirectamente.

- Altura: es la longitud del camino más largo desde una determinada transacción hasta el principio.

- Profundidad: es la longitud del camino más largo desde el principio hasta una transacción definida.

3.2. Funcionamiento

Tres pasos son suficientes para ejecutar una transacción en IOTA:

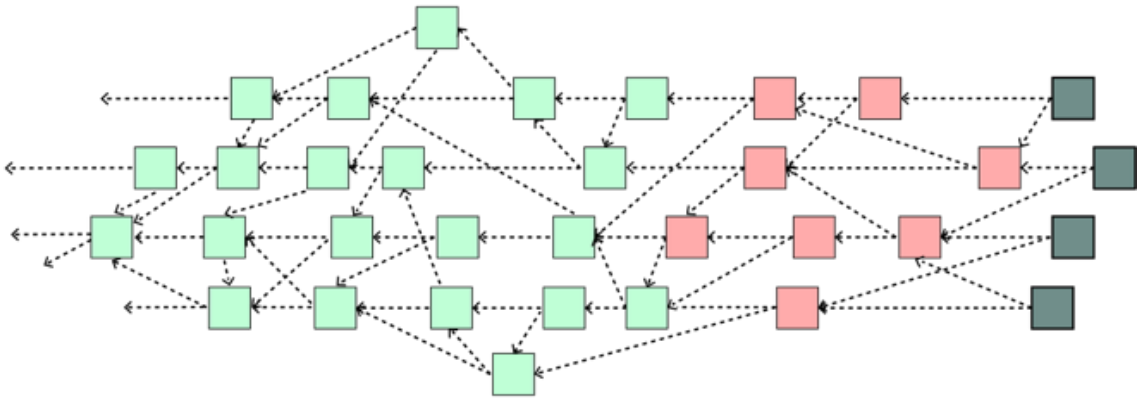
- Firma: la transacción se firma con claves privadas.

- Selección de punta: se seleccionan dos bloques no confirmados con el algoritmo Monte-Carlo Markov y se hacen referencia en la nueva transacción.

- Prueba de trabajo: para confirmar la transacción, el remitente tiene que pasar un algoritmo de prueba de trabajo que es similar al algoritmo de Bitcoin.

Una vez que esto se logra, la transacción es válida. Luego, alguien más hará referencia a esta transacción para confirmarla.

Figura 1. **Estructura Tangle**



Fuente: *IOTA (protocolo).* https://es.m.wikipedia.org/wiki/IOTA_(protocolo). Consulta: 7 de octubre de 2019.

En la figura, se representa la red de transacciones del Tangle, la descripción es la siguiente:

- Bloques verdes: transacciones que ya están confirmadas por la red, que ya están en consenso.

- Bloques rosados: transacciones en las que todavía no se está seguro de su aceptación.

- Bloques grises: transacciones denominadas tips, son transacciones no confirmadas.

El objetivo de cualquier transacción es estar a la izquierda, que una transacción sea confirmada y aceptada por toda la red, de llegar a un consenso. Se llega a un consenso cuando todos los nodos trabajan en conjunto para validar las transacciones.

En la figura 1, la principal diferencia de los bloques de la izquierda y los bloques del medio es que todos los bloques de la derecha hacen referencia indirectamente a los bloques que están delante de ellos. Para cada transacción confirmada, hay una ruta directa que conduce a ella desde una sugerencia. Como tal, es bastante fácil determinar el nivel de confirmación de una transacción.

En esta estructura no hay límite del tiempo, debido a que todas las transacciones nuevas no esperan a que exista un minado de otras transacciones que pertenecen a un bloque establecido, a causa de que no existen bloques.

3.2.1. Prueba de trabajo

Para validar una transacción será necesario realizar una prueba de trabajo (PoW). Esto consta de la resolución de un problema de cálculo matemático que implica conseguir un *hash* de manera aleatoria como resultado.

Para realizar la PoW se toman los valores que componen una transacción:

- Dirección: es la ubicación del monedero de destino, quien recibe los *tokens*.
- Etiqueta: es una etiqueta para organizar la clase de transacción, es informativa.
- Marca de tiempo: fecha de la transacción.
- Valor: el número de *tokens* que se transfieren.
- Índices: valores enteros que representan las transacciones actuales en un paquete.

- Fragmento de mensaje de firma: texto que puede ser utilizado como mensajería dentro de la transacción, puede contener valores nulos, números o mensajes.
- Transacción *trunk* y *branch*: tienen los valores *hash* de la transacción previa que ha sido aprobada y la actual.

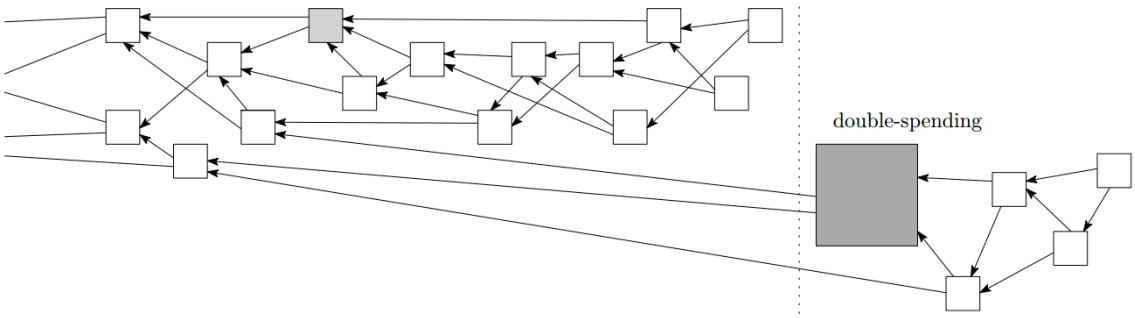
3.3. Escalabilidad

Tangle es perfecto para un libro mayor distribuido, donde innumerables dispositivos están conectados. Además, Tangle almacena en caché los pesos de las transacciones en subtangles, para combinarlos con las transacciones validadas recientemente. Otra característica de Tangle, es contar con las transacciones múltiples. Están hechos de un número diverso de transacciones encadenadas mientras se usa la misma dirección. Además, estas cadenas están configuradas para que solo la primera transacción tenga valor, mientras que todas las siguientes transacciones tienen un valor cero.

3.4. Identificación y solución de problemas

Existe un problema en el Tangle, llamado doble gasto. Es una situación en la que los usuarios envían más *iotas* del que tienen en dos o más transacciones. Incluso si cada transacción individual del usuario está cubierta por el saldo de la cuenta y una de estas transacciones sería inválida, ambas transacciones no son válidas juntas. Incluso en este caso, estas transacciones no se confirmarían porque no es posible un saldo negativo de la cuenta.

Figura 2. **Problema doble gasto**



Fuente: POPOV, Serguei. *The Tangle*. p. 16. Consulta: 8 de octubre de 2019.

Un doble gasto es un intento exitoso de ganar ‘una carrera contra el tiempo’ para confirmar una transacción que utiliza el mismo saldo que se prometió al receptor original pero que también se enviará a un segundo receptor para estafar al anterior.

Al hacerlo, se finge completar una transacción y se muestra cómo se confirma en una billetera, pero con el tiempo y la carrera por ganar más peso, la transacción se vuelve inválida, a favor de la segunda transacción que se hizo simultáneamente.

Eso significa que se puede negociar y recibir el valor equivalente en valor de los *iotas* de esa transacción de doble gasto, pero después de un corto tiempo, se poseerá ambos: los propios fondos de vuelta más el activo negociado del socio comercial. Esto significaría que IOTA no funciona, las personas nunca tuvieron el 100 % de garantía de que están en posesión de sus fondos o de los activos negociados que dieron por *iotas*.

Y como resultado: IOTA ciertamente caería en valor, las personas y las empresas perderían confianza y al final, IOTA ciertamente sufriría una reputación duradera. Este ataque podría usarse en los mercados comunes, para debilitar IOTA y realizar un gran gasto doble, para obtener un gran beneficio de la reacción de los mercados.

IOTA trata el siguiente problema usando el algoritmo de camino aleatorio para seleccionar los bloques no confirmados más grandes y significativos. El consenso se basa en la pregunta de qué transacción es válida. Otro problema surge para los destinatarios, porque necesitan saber si realmente han recibido el envío.

En el Tangle, este problema se resuelve con un concepto llamado confirmación de confianza. La confianza de confirmación se calcula ejecutando el mecanismo de selección para las sugerencias 100 veces. El número de casos en los que estos consensos confirman la transacción se divide por 100 para calcular la confianza de confirmación.

Los bloques no confirmados no se tratan de la misma manera, pero los bloques con mayores probabilidades tienen más importancia. Si hay cierta confianza en una transacción, es probable que se llegue a un consenso al respecto. Sin embargo, existe una probabilidad residual de que sean rechazados.

Cuando existen transacciones conflictivas, los nodos deben decidir qué transacciones quedarán huérfanas. Para eso se utilizan los algoritmos de equilibrio.

3.4.1. Algoritmo de camino aleatorio

Es un algoritmo que proporciona rutas aleatorias en un gráfico. Una caminata aleatoria significa que se comienza en un nodo, se elige un vecino para navegar al azar o en función de una distribución de probabilidad proporcionada y luego se vuelve a ejecutar lo mismo desde ese nodo, manteniendo la ruta resultante en una lista.

3.4.2. Algoritmo Markov-Chain Monte Carlo

Es un método matemático que extrae muestras al azar de una caja negra para aproximar la distribución de probabilidad de los atributos en un rango de objetos, por ejemplo, la altura de los hombres, los nombres de los bebés, los resultados de eventos como el lanzamiento de monedas, etc. Se podría decir que es un método estadístico a gran escala para adivinar y verificar. El método hace referencia al casino de Monte Carlo, es la capital del juego del azar, ya que genera números aleatorios.

3.4.3. Algoritmo Nash

Es un concepto de teoría de juegos que determina la solución óptima en un juego no cooperativo en el que cada jugador no tiene ningún incentivo para cambiar su estrategia inicial. Bajo el equilibrio de Nash, un jugador no gana nada al desviarse de la estrategia elegida inicialmente, suponiendo que los otros jugadores mantengan sus estrategias sin cambios. Un juego puede incluir múltiples equilibrios de Nash o ninguno de ellos.

Conceptualiza el comportamiento y las interacciones entre los participantes del juego para determinar los mejores resultados. También,

permite predecir las decisiones de los jugadores si están tomando decisiones al mismo tiempo y la decisión de un jugador tiene en cuenta las decisiones de otros jugadores.

3.5. Transacciones *offline*

La razón principal por la que se creó IOTA es para habilitar y ser la columna vertebral del internet de las cosas. Los desarrolladores imaginan un futuro en el que los dispositivos intercambien recursos y servicios entre ellos sin la participación de ningún tercero. A medida que el internet de las cosas comience a desarrollarse, la necesidad de la descentralización inteligente es evidente.

La belleza de Tangle es que puede ramificarse y volver a conectarse a la red de manera fluida. Esta partición es clave para adaptarse a los requisitos rigurosos de un entorno de internet de las cosas asíncrono.

3.6. Subtangles

Son tangles separados con transacciones, que pueden unirse al Tangle principal en un momento posterior. Un subtangle no puede recibir hitos, por lo tanto, la validación de las transacciones se basa solo en la probabilidad.

Si un día, el subtangle se vuelve a conectar con el Tangle principal: todas sus transacciones se verán como no confirmadas porque ninguna transacción de hito las está validando. Para que se confirmen esas transacciones, los nodos completos previamente en el subtangle deben retransmitir todas esas transacciones al Tangle principal para que el coordinador las valide.

3.7. Resistencia cuántica

Como se mencionaba en la descripción de Tangle, el código ternario es más eficiente que el código binario, ya que tiene un menor consumo de energía para realizar las operaciones, el problema es que se necesita cambiar el sistema de computadoras. Es aquí donde entra en juego la computación cuántica.

3.7.1. Computación cuántica

La computación cuántica será el fin del cifrado, tal como lo conocemos. En el contexto de la interconexión global de IoT, es un problema que exige una solución segura. IOTA tiene un algoritmo integrado de resistencia cuántica, el esquema de firma única de Winternitz. El *hash* de Winternitz se conoce como una firma post-cuántica porque los ataques cuánticos no reducen significativamente la seguridad dada por este *hash*.

“La unidad fundamental de información en computación cuántica es el qubit. Los qubits son, por definición, sistemas cuánticos de dos niveles. Las computadoras cuánticas aprovechan los efectos físicos, como entrelazamiento y superposiciones de estados, para realizar procesos computacionales”[2].

Si bien la gama de aplicaciones potenciales de las computadoras cuánticas es amplia, la más relevante en el contexto de la tecnología Blockchain y la criptografía en general es la capacidad de ejecutar algoritmos específicos a una velocidad inmensamente superior que cualquier supercomputadora existente.

[2] ALLENDE, Marcos. *¿Cómo funciona la computación cuántica?* https://blogs.iadb.org/conocimiento-abierto/es/como-funciona-la-computacion-cuantica/. Consulta: 15 de octubre de 2019.

Cuando se trata del futuro de IoT, se tendrán millones de transacciones. Entrando lentamente en las necesidades de transacciones en tiempo real, la mayoría de las soluciones de Blockchain disponibles no se escalarían, ya que no podrán escalar a un mayor número de transacciones por segundo y al mismo tiempo proporcionar una infraestructura estable y ejecutarse en un hardware liviano.

El proceso de encontrar un *nonce* (número aleatorio usado en Blockchain) para generar un bloque de Bitcoin es un buen ejemplo de un problema de *spam*. A partir de hoy, en promedio se debe verificar alrededor de 2 ^ 68 bloques, para encontrar un *hash* adecuado que permita generar un bloque. Una computadora cuántica necesitaría operaciones O (sqrt (N)) para resolver un problema del tipo anterior que necesita operaciones O (N) en una computadora clásica.

Por lo tanto, una computadora cuántica estaría alrededor de sqrt (2 ^ 68) = 2 ^ 34, esto es aproximadamente 17 mil millones de veces más eficiente que la minería Bitcoin actual. Además, vale la pena señalar, si Blockchain no aumenta su dificultad en respuesta a un mayor poder de *hashing*, eso conduciría a una mayor tasa de bloques sueltos.

Uno de los supuestos casos de uso más ampliamente discutidos es ejecutar el famoso algoritmo de Shor para la descomposición de factores, lo que podría volver obsoletas muchas técnicas de cifrado contemporáneas. Bitcoin utiliza criptografía de curvas elípticas. Es teóricamente posible realizar un ataque de fuerza bruta en cualquier billetera de Blockchain, esto debido a que los saldos son públicos en Blockchain y que existe un incentivo económico para hacerlo.

El ataque había reducido la complejidad de O (N) a O (sqrt (N)). Es un ataque difícil de hacer y depende de un poco de suerte. Pero es suficiente que se para demostrar que la criptografía de curvas elípticas tiene una debilidad.

Estas propiedades de la computación cuántica pueden servir para aplicar ataques cibernéticos a Blockchain, ataques DDoS para robar datos o saldos de las cuentas de los usuarios, craquear firmas digitales o minar bitcoins.

3.7.2. Algoritmos cuánticos

El objetivo de los algoritmos cuánticos es realizar operaciones que hace la computación actual de una forma óptima, en utilizar menos tiempo y recursos. Para esto, se deben explotar las propiedades cuánticas de los *qubits*, para ejecutar los algoritmos cuánticos más utilizados usados, los cuales son:

3.7.2.1. Algoritmo de Shor

Es un algoritmo conceptual de computadora cuántica optimizado para resolver factores primos. Toma un factor, *n* para genera sus factores. Es mágico encontrarse con reducir la cantidad de pasos necesarios para encontrar los factores primos de un número. El algoritmo se divide en dos partes:

- Una reducción del problema de factorización al problema de búsqueda de orden, esto se puede realizar hoy en una computadora clásica.

- Un algoritmo cuántico para resolver el problema de búsqueda de orden, este es ineficaz debido a la falta de capacidades de computación cuántica.

El algoritmo de Shor es probabilístico, tiene una alta probabilidad de que la respuesta sea exitosa; mientras que la probabilidad de fallo puede ser disminuida repitiendo el algoritmo.

3.7.2.2. Algoritmo de Grover

El algoritmo de Grover permite a un usuario buscar elementos específicos en una lista desordenada. El algoritmo de Grover es probabilístico: mide las probabilidades de varios estados potenciales del sistema. Una computadora cuántica usaría el algoritmo de Grover para realizar varias rondas de computación. A través de cada ronda de cómputo, aumenta la probabilidad de que ciertos artículos tengan la condición deseada. El algoritmo reduce las selecciones a medida que avanza y muestra un resultado de alta probabilidad al final.

3.8. Funciones *hash*

IOTA ha acrecentado su seguridad utilizando una función *hash* llamada Troika. Troika es una función de cifrado *hash* que funciona en mensajes ternarios para su uso en la tecnología de contabilidad distribuida de IOTA diseñada por CYBERCRYPT. Esta página ofrece una visión general del diseño de Troika y proporciona material como el documento de referencia y la implementación.

Las características principales de Troika son:

- Permutación diseñada para plataformas ternarias
- Construcción a base de esponja
- Longitud de salida de 243 trits

- Nivel de seguridad de 243 trits para imágenes, 243/2 trits para colisiones

En la actualidad, se cree que es robusto contra la mayoría de los ataques, incluidos el criptoanálisis diferencial y lineal, las propiedades de difusión, los ataques de encuentro en el medio, los ataques algebraicos y los ataques invariantes.

4. TECNOLOGÍA BLOCKCHAIN

4.1. Descripción

Blockchain fue introducido por primera vez por Satoshi Nakamoto y es el diseño subyacente para las transacciones de Bitcoin. En términos más simples, Blockchain es una tecnología de base de datos, un libro mayor distribuido de registros que puede seguir creciendo en tamaño. Los registros pueden ser bitcoins, contratos inteligentes o cualquier otra entrada. Estos se combinan en los llamados bloques.

Blockchain permite una total transparencia, seguridad y autenticidad de la información. La arquitectura Blockchain consta de varios nodos que son computadoras conectadas a la red. Cada nodo obtiene una copia de Blockchain que se puede descargar.

Alterar una información sobre Blockchain es difícil, por lo tanto, esto lo hace extremadamente seguro. Cada bloque se agrega a través de la criptografía, lo que dificulta la manipulación de datos. Blockchain se introdujo por primera vez para bitcoins y luego varias altcoins decidieron utilizar este sistema. Inicialmente, el objetivo era asegurar las transacciones digitales. Sin embargo, Blockchain ha demostrado tener un potencial inmenso para ser utilizado para varios otros propósitos.

Blockchain se puede usar en varios campos, como banca, pago y transferencia de dinero, préstamos, micropagos, administración de identidad,

redes, pronósticos, arrendamiento y venta de automóviles, educación, ciberseguridad, seguimiento del dinero de los contribuyentes.

4.2. Funcionamiento

En términos simples, Blockchain se puede considerar como una base de datos distribuida. Las adiciones a esta base de datos son iniciadas por uno de los miembros, es decir, los nodos de la red, estos crean un nuevo bloque de datos que puede contener todo tipo de información. Este nuevo bloque se transmite a todas las partes de la red utilizando criptografía para que los detalles de la transacción no se hagan públicos.

Los otros nodos de la red determinan colectivamente la validez del bloque de acuerdo con un mecanismo de consenso. Una vez validado, el nuevo bloque se agrega a la cadena de bloques, lo que esencialmente resulta en una actualización del libro de transacciones que se distribuye a través de la red.

Cada usuario en una red Blockchain tiene un conjunto de dos claves. Una clave privada, que se utiliza para crear una firma digital para una transacción y una clave pública, que es conocida por todos en la red. La clave pública sirve como dirección en la red Blockchain; también se utiliza para verificar una firma digital y validar la identidad del remitente.

Figura 3. **Funcionamiento Blockchain**

Fuente: *Blockchain: la transferencia de datos digitales no centralizada.* https://blog.mdcloud.es/blockchain-la-transferencia-datos-digitales-no-centralizada/. Consulta: 11 de octubre de 2019.

4.3. Principales criptomonedas

Las principales criptomonedas desarrolladas bajo la tecnología Blockchain son:

4.3.1. Bitcoin

Es la criptomoneda más popular del mundo. Bitcoin generalmente se describe como una moneda virtual, descentralizada y anónima que no está respaldada por el gobierno o respaldada por ninguna otra entidad legal y que no puede intercambiarse por oro u otro producto.

Bitcoin se basa en un mecanismo de consenso de prueba de trabajo. El problema de bitcoins se lleva a cabo a través de un proceso llamado minería. Dicho proceso, cuyos elementos completos están disponibles públicamente a través de software de código abierto, implica que las personas voluntariamente trabajen en sus propias computadoras a disposición de la red de Bitcoin para resolver problemas matemáticos complejos. Las computadoras que pueden resolver tales problemas creando bloques de transacciones, por estas acciones son recompensados con bitcoins.

El número total de bitcoins que se pueden crear a través de la minería es limitado: el sistema Bitcoin está programado para que el desarrollo de bloques en el tiempo se recompense con cada vez menos bitcoins y que en ningún momento existan más de 21 millones de bitcoins. El hecho de que la creación y el aumento de bitcoins esté automatizado y limitado por el sistema implica que no es necesaria la intervención de una entidad para emitir bitcoins.

El número limitado de bitcoins, junto con el hecho de que las tasas de conversión para bitcoins están determinadas por la oferta y la demanda, sin que un organismo gubernamental pueda intervenir, resulta en una alta volatilidad en los precios de bitcoins.

4.3.2. Ethereum

Ethereum es la segunda criptomoneda más popular en el mercado, es una plataforma descentralizada que está desarrollada bajo la tecnología Blockchain. Ethereum, lanzado en julio de 2015, es una plataforma descentralizada que ejecuta los llamados contratos inteligentes; también, funciona como un medio de intercambio.

Los contratos inteligentes son contratos o aplicaciones de auto ejecución, esto significa que se ejecutan exactamente como se programaron sin ninguna posibilidad de tiempo de inactividad, censura, fraude o interferencia de terceros. Éter permite la creación de contratos inteligentes en la plataforma Ethereum, también funciona como un medio de intercambio.

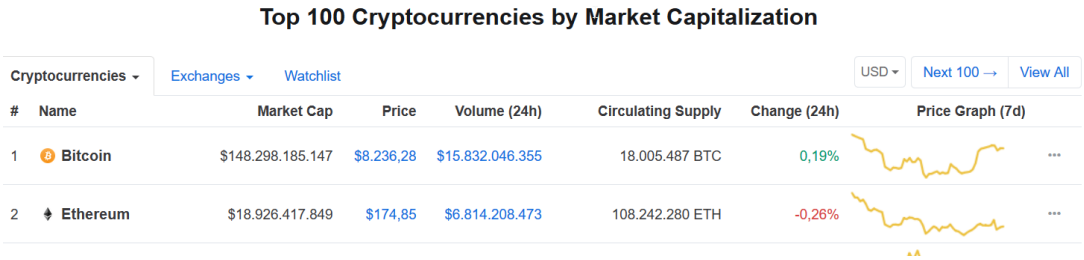
En términos simples, Ethereum es muy parecido a un sistema operativo de teléfono inteligente sobre el cual se pueden construir aplicaciones de software. Técnicamente hablando, la plataforma Ethereum en sí misma no es una criptomoneda. Sin embargo, al igual que otras cadenas de bloques abiertas y sin permiso, Ethereum requiere una forma de valor en la cadena para incentivar la validación de transacciones dentro de la red, es decir, una forma de pago para los nodos de la red que ejecutan las operaciones.

4.3.3. Altcoin

Las Altcoins son criptomonedas, excepto los bitcoins. Altcoins significa monedas alternativas. Actualmente hay más de cientos de altcoins disponibles en el mercado. Estas son alternativas de Bitcoin y varían en funcionalidad básica. Se predice que algunas altcoins pueden impulsar el mercado de Bitcoin.

Existen casi 478 monedas alternativas. Cabe la posibilidad de reparar cualquier defecto de diseño de Bitcoin mientras se construyen altcoins más nuevos. La arquitectura básica de Blockchain para estas altcoins sigue siendo la misma.

Figura 4. **Criptomonedas más populares**



Fuente: *Top 100 cryptocurrencies by Market Capitalization.* https://coinmarketcap.com/. Consulta: 12 de octubre de 2019.

4.4. Características

Las principales características de Blockchain son:

4.4.1. Minería de datos

Significa al conjunto de pasos necesarios para certificar y gestionar las transacciones de una criptomoneda. En esto, un minero está involucrado. El minero es responsable de resolver un problema matemático por el cual el minero será recompensado con criptomonedas. El minero tiene que proporcionar una prueba de trabajo. Como prueba de trabajo, el minero tiene que encontrar un número llamado nonce. Sin embargo, esto debe ser aceptado en toda la red por otros mineros.

4.4.2. Minería en la nube

La minería de nube brinda a las personas la capacidad de adquirir capacidad de minado de hardware vía remota por un contrato de tiempo.

Básicamente, es un alquiler de un equipo o centro de cómputo para minar, ya que se evita la compra de hardware y software.

Las ventajas de este esquema es que no se debe comprar equipo de cómputo robusto, se evita el gasto de recursos para sistemas de ventilación y gasto en electricidad.

Las desventajas es la conexión a internet, sin internet no se puede utilizar esta vía remota, también posibilidad de fraude, ya que no se puede comprobar la existencia del centro de cómputo que renta el equipo.

4.4.3. Protección de datos en Blockchain

En lugar de una cuenta física o en línea que debe ser mantenida por un tercero, como un banco, cada unidad de Bitcoin se almacena en la propia cadena de bloques. Los usuarios pueden acceder de forma segura a bitcoins utilizando sus pares de claves privadas o públicas.

Un consumidor puede gastar o transferir sus bitcoins solo usando sus claves privadas, mientras que un comerciante puede recibir bitcoins compartiendo sus claves públicas con el consumidor. Una vez que la transacción ha sido retransmitida a través de internet e incluida en un bloque, se considera permanente. El comerciante puede reclamar irrefutablemente la propiedad de esos bitcoins. También, puede usar sus propias claves privadas para gastar esos bitcoins.

4.4.4. Sistema de confianza

En la mayoría de los sistemas de pago tradicionales, las transacciones no solo dependen de las dos partes involucradas, sino también de un intermediario, como un banco, una compañía de tarjetas de crédito o un proveedor de pagos. Cuando se usa la tecnología Blockchain, esto ya no es necesario porque la red distribuida de nodos verifica las transacciones a través de la minería. Por esta razón, Blockchain a menudo se conoce como un sistema de confianza

Por lo tanto, un sistema Blockchain elimina el riesgo de confiar en una sola organización y también reduce los costos generales y las tarifas de transacción al eliminar intermediarios y terceros.

4.4.5. Tecnología descentralizada

Blockchain es un sistema descentralizado que significa que ninguna autoridad central puede tomar el control del sistema. El valor central de Blockchain es que permite que una base de datos se pueda compartir directamente sin un administrador central. Blockchain puede eliminar el costo de contratar personas expertas para prevenir o detener los ataques en el sistema mediante el uso de la criptografía.

4.4.6. Transparencia

Cualquier información en la cadena de bloques puede ser visible para cualquier persona, también si se realizaron cambios en la cadena de bloques, esos cambios son visibles públicamente. Por eso, Blockchain se usa en criptomonedas porque cada transacción se registra y se muestra al público.

4.5. Problemas con algoritmos cuánticos

Una de las desventajas de Blockchain es la incapacidad de protegerse ante los algoritmos cuánticos, esto es debido al uso del sistema binario en las computadoras actuales. Comparando la velocidad de procesamiento de la información entre las computadores actuales y cuánticas es aproximadamente cien millones de veces más rápida las computadoras cuánticas. La capacidad de la computación cuántica para descodificar y quebrantar los esquemas de criptografía clásica es inmensa, en la década de los 90, se ejecutó el algoritmo cuántico de Shor rompiendo varios esquemas criptográficos.

Si el algoritmo de Shor fue capaz de romper la seguridad de Blockchain, se puede asumir que otro algoritmo cuántico, como el de Grover, también será capaz.

Blockchain consta de nodos encriptados conectados en una cadena, lo que actualmente hace que sea casi imposible de hackear. El orden de las entradas se adhiere al protocolo Blockchain, lo que lo hace resistente a la falsificación.

Para hackear con éxito una cadena de bloques, se necesitaría alterar tanto el bloque objetivo como todos los bloques conectados. Las cadenas de bloques se sincronizan a través de una red de igual a igual. En este tipo de sistema, no existe un punto central de falla para que los piratas informáticos penetren. para que un hacker tenga la posibilidad de penetrar en la red, necesitaría alterar simultáneamente al menos el 51 % de la cadena de bloques.

La computación cuántica, a diferencia de la computación tradicional, utiliza factoriales y exponenciales en algoritmos. No se limitan a ecuaciones lineales

porque pueden calcular algoritmos con exponenciales debido a que utilizan el sistema ternario. Esta innovación permite a los sistemas resolver problemas más rápidamente con el tiempo.

Por lo tanto, Blockchain no estará listo para tal avance. La computación cuántica podría ser catastrófica para todo el historial de transacciones.

4.6. Otras desventajas

- Una desventaja de Blockchain es que una vez que los datos se han agregado a la cadena de bloques, es muy difícil modificarla. Si bien la estabilidad es una de las ventajas de Blockchain, no siempre es buena. Cambiar los datos o el código de Blockchain suele ser muy exigente, requiere una bifurcación donde se abandona una cadena y se toma una nueva.

- Otra desventaja de Blockchain es que utiliza criptografía de clave pública para dar a los usuarios la información sobre sus unidades de criptomonedas. Cada dirección de Blockchain tiene una clave privada correspondiente. Si bien la dirección se puede compartir, la clave privada debe mantenerse en secreto. Los usuarios necesitan su clave privada para acceder a sus fondos, lo que significa que actúan como su propio banco. Si un usuario pierde su clave privada, el dinero se pierde efectivamente y no hay nada que pueda hacer al respecto.

- Las cadenas de bloques, especialmente aquellas que usan prueba de trabajo, son altamente ineficientes. Como la minería es altamente competitiva y solo hay un ganador cada diez minutos, el trabajo de todos los demás mineros se desperdicia. A medida que los mineros

continuamente intentan aumentar su poder de cómputo, eso hace que los recursos utilizados por la red Bitcoin hayan aumentado significativamente en los últimos años, actualmente los países europeos consumen más energía que muchos países.

- Los libros de contabilidad de Blockchain pueden crecer mucho conforme pasa el tiempo. La cadena de bloques de Bitcoin actualmente requiere alrededor de 200 GB de almacenamiento. El crecimiento actual en el tamaño de Blockchain parece estar superando el crecimiento en los discos duros y la red corre el riesgo de perder nodos si el libro mayor se vuelve demasiado grande para que las personas lo descarguen y almacenen.

4.7. Futuro de Blockchain

Se espera que el mercado global de Blockchain sea de $ 20 mil millones para 2024. Las características positivas de Blockchain, como la transparencia, la integridad, la confidencialidad, la flexibilidad y la seguridad, se pueden utilizar para aprovechar y facilitar la actividad comercial, creando así nuevas empresas comerciales.

Muchas grandes empresas como IBM y Microsoft están comenzando nuevas empresas para Blockchain. Casi el 90 % de los principales bancos de América del Norte y Europa están explorando soluciones basadas en Blockchain. Un mito común es que Blockchain eliminará varios trabajos. El hecho es que debido al crecimiento de Blockchain en Internet, algunos trabajos quedarán obsoletos. Sin embargo, se abrirán nuevas empresas de trabajo como resultado de la transformación de Blockchain.

5. COMPARACIONES ENTRE TECNOLOGÍAS Y CRIPTOMONEDAS

5.1. Tangle vs Blockchain

Las dos tecnologías se basan en la criptografía, pero esto es lo único que las une. Tangle y Blockchain tienen más diferencias que similitudes. Blockchain se basa en tener la cadena de bloques linealmente donde cada registro siguiente verifica el anterior y comprende la información sobre todas las transacciones realizadas antes. El mantenimiento del sistema los mineros. Cada usuario de Blockchain necesita tener la versión actualizada válida del libro público. Así es como funciona Bitcoin, hasta ahora, ha sido la criptomoneda más efectiva y exitosa.

Este sistema tiene sus altibajos. El tamaño del bloque es limitado y la cantidad de bloques creados cada hora también es limitada. El libro mayor se hace más grande y la tarea de minar se vuelve más difícil, lo que conduce a mayores recompensas de bloque. Por lo tanto, el sistema se vuelve más lento y caro.

Las nuevas ideas criptográficas siguen los pasos de la cadena de bloques e incluso afirman que son el futuro de la criptografía. El enfoque DAG significa que el libro mayor se distribuye entre todos los usuarios, no solo los mineros. En realidad, se puede decir que no existen mineros aquí o que todos los participantes de la red son mineros. Por esta razón, el sistema se vuelve más poderoso con cada nuevo usuario. Mientras Tangle recibe más transacciones, no se vuelve más lento ni pesado, ya que cada nuevo registro en el libro mayor

contiene el mismo volumen de información que el anterior. Solo necesita verificar dos transacciones, sin la necesidad de mantener toda la red.

Una de las grandes comparaciones entre las dos tecnologías es la velocidad de transacción y las tarifas por ellas. A medida que la estructura de los registros de datos en las dos redes difiere, estas variaciones conducen a una mayor desigualdad en el costo y el tiempo de las transacciones.

Un minero tiene que verificar la transferencia de Bitcoin y agregar el bloque al libro mayor a través es un problema matemático difícil. Cuanto más grande es la cadena de bloques, más difícil se vuelve. Los mineros son incentivados por el sistema de tarifas, pero aquí radica uno de los principales problemas de Bitcoin. Cuando las tarifas son altas, hay más mineros para mantener la red, en teoría, esto es bueno. Sin embargo, los usuarios de Bitcoin quieren tarifas más bajas para realizar transacciones.

Si las tarifas de las transacciones son bajas, la recompensa del minero es baja. Muy pocos mineros quieren hacer ese trabajo. Por lo tanto, en la red Bitcoin, se tienen transacciones que son demasiado lentas o caras.

Por el contrario, con Tangle, los usuarios no reciben ninguna tarifa por verificar las transacciones. Al enviar IOTA, debe confirmar dos transacciones elegidas por el algoritmo, la tarea es solo asegurarse de que no entren en conflicto entre sí. También debe resolver una tarea criptográfica, pero no afecta el acuerdo sobre el historial completo de todas las transacciones realizadas anteriormente, como en Bitcoin. Por lo tanto, la tarea es mucho más fácil y el tiempo que lleva es mucho más corto. Esta es la razón por la cual las criptomonedas basadas en DAG son gratuitas y funcionan mucho más rápido que las de Blockchain.

Para hacer un resumen de las dos tecnologías se utiliza la siguiente tabla:

Tabla II. **Comparación Tangle vs Blockchain**

	Tangle	**Blockchain**
Escalabilidad	Más fluido y escalable, conforme pasa el tiempo es más rápido y poderoso.	Se vuelve más lento y menos productivo mientras pasa el tiempo.
Tarifas	Es gratis, no tiene recompensan en bloque y los nodos no necesitan tarifas para verificar las transacciones.	Las tarifas son muy altas y se debe pagar un precio irrazonable o faltan mineros y se debe esperar demasiado tiempo para transferir dinero.
Confianza	No se ha demostrado una verdadera efectividad ni confianza.	Es totalmente confiable.
Descentralización	Si más de la tercera parte de toda la potencia informática que facilita la red está controlada por una persona o entidad, podrán piratearla y realizar transacciones falsas.	Una de las partes podría controlar más del 50 % de todo el poder de *hashing* de la cadena de bloques.
Seguridad	Aún no es seguro ni confiable, los creadores de IOTA mencionan que se eliminará este problema conforme pase el tiempo de forma natural a medida que la red crezca.	Debido al lento y complicado proceso de verificación en la cadena de bloques garantiza que nadie controle el 50 % de los nodos.
Resistencia cuántica	Utiliza algoritmos criptográficos que son resistentes a los ataques cuánticos.	Es susceptible a los ataques cuánticos.

5.1.1. Ataques cibernéticos

En IOTA un ataque del 34 % puede ocurrir, cuando un atacante posee el 34 % de la potencia de procesamiento total puede crear transacciones maliciosas. IOTA depende de un coordinador hasta que sea lo suficientemente grande como para reducir la posibilidad de un ataque del 34 % prácticamente a cero.

El coordinador verifica las transacciones existentes y es entrenado para recuperar IOTA cuando es atacado. Esto se da en un escenario hipotético en el que la red es tomada por alguien que une más del 34 % del *hashrate* de toda la red. El *hashrate* es la potencia informática de una red. Esta protección solo estaría garantizada si un número suficientemente grande de dispositivos y usuarios se unen a la red.

En Blockchain se llama el ataque del 51 %, este se refiere a un ataque a una cadena de bloques, generalmente Bitcoin, por un grupo de mineros que controlan más del 50 % del *hashrate* de la red. Los atacantes podrían evitar que las nuevas transacciones obtengan confirmaciones, lo que les permitirá detener los pagos entre algunos o todos los usuarios. También, podrían revertir las transacciones que se completaron mientras controlaban la red, lo que significa que podrían gastar el doble de monedas.

Cambiar los bloques históricos sería extremadamente difícil incluso en el caso de un ataque del 51 %. Cuanto más atrás estén las transacciones, más difícil será cambiarlas. Sería imposible cambiar las transacciones antes de un punto de control, más allá de las cuales las transacciones están codificadas en el software de Bitcoin.

5.2. IOTA vs Bitcoin

Las similitudes y diferencias entre estas criptomonedas son:

5.2.1. Puntos en común entre IOTA y Bitcoin

IOTA y Bitcoin son pioneros en sus respectivos campos. Si bien Bitcoin fue la primera aplicación distribuida de Blockchain, IOTA fue la primera

aplicación distribuida para Tangle. También, fueron pioneros en sus casos de uso: Bitcoin para monedas digitales e IOTA como columna vertebral para internet de las cosas.

5.2.2. Diferencias entre IOTA y Bitcoin

IOTA se basa en un gráfico acíclico dirigido mientras que Blockchain no. IOTA no tiene proceso de minería ni tarifas de transacción. Si bien Bitcoin tiene un límite de siete transacciones por segundo, IOTA se escala infinitamente, algo que Bitcoin nunca podría lograr. IOTA no está diseñado para ser una criptomoneda única; está diseñado para conectar otras aplicaciones a través del internet de las cosas. IOTA también es desarrollado por una fundación sin fines de lucro.

5.3. IOTA vs Ethereum

Las similitudes y diferencias entre estas criptomonedas son:

5.3.1. Puntos en común entre IOTA y Ethereum

IOTA comparte los mismos puntos en común con Ethereum que con Bitcoin. Ethereum es una plataforma Blockchain pionera en su campo y creó una estructura muy propia. Su caso de uso se asemeja ligeramente al de IOTA: quiere habilitar contratos inteligentes, que puede reemplazar los contratos de seguro. La gran cantidad de dispositivos e información se puede procesar con cadenas de bloques privadas.

5.3.2. Diferencias entre IOTA y Ethereum

IOTA tiene tarifas de transacción mucho más bajas; puede enviar casi de inmediato una confirmación y tiene escalabilidad. En Ethereum, la red suele estar congestionada, lo que significa que los pagos no se realizan de inmediato o el usuario paga más. Para confirmar las transacciones, Ethereum usa prueba de trabajo, pero quiere cambiar a prueba de participación en algún momento en el futuro. La prueba de participación pondría fin a la minería.

Ethereum es la plataforma para su propio *token* llamado ether, en el que se ejecutan los contratos.

6. APLICACIONES UTILIZANDO IOTA

6.1. IOTA y el internet de las cosas

Internet de las cosas es el ángulo principal para IOTA. Este término es una visión para que los dispositivos y sensores conectados puedan interactuar directamente con cada uno sin necesidad de otro ser humano. Por ejemplo, las cámaras inteligentes procesen datos en tiempo real, las redes electrónicas inteligentes o incluso los productos relacionados con la salud puedan enviar datos sobre comportamientos.

IOTA se relaciona perfectamente con el internet de las cosas ya que deben considerar las necesidades especiales de los sensores y dispositivos en este ecosistema, las relaciones entre ellos están en común en los siguientes puntos:

- Ligero: cuando un programa o herramienta se conecte a otros debe ser lo más ligero posible y sin funciones innecesarias.

- Sin tarifas de transacción: para permitir la comunicación entre dispositivos IoT sin problemas debe ocurrir sin tarifas. De todas formas, es lógico, ya que los dispositivos no podrían pagar.

- Escalabilidad: al contrario de las tecnologías Blockchain actuales, el protocolo debe ser escalable; no debe haber un límite de cuántas transacciones puede procesar por segundo. El internet de las cosas se define por la masa de dispositivos y datos.

- Apertura: las acciones deben ejecutarse fácilmente, especialmente para dispositivos IoT, es importante, conectarse a través de Bluetooth u otros estándares.

Las tecnologías actuales de Blockchain no ofrecen esto. Son demasiado lentas y complicadas para este caso y la columna vertebral futura de internet de las cosas debe cumplir estos requisitos o no es una columna vertebral. Las transacciones no confirmadas que se acumulan en la red, como en el caso de Bitcoin, obstruyen la red y la hacen menos utilizable. El internet de las cosas se caracteriza por la gran cantidad de dispositivos, por lo que su columna vertebral necesita escalar.

Figura 5. **IOTA y el internet de las cosas**

Fuente: PEÑA, Eddyver. *Internet de las cosas.* https://www.pinterest.com/eddyver1967/internet-de-las-cosas/. Consulta: 19 de octubre de 2019.

6.2. Procesador Jinn

Muchas personas han invertido en IOTA porque es una gran solución de software que ya están adoptando las grandes empresas debido a sus ventajas en velocidad, escalabilidad y falta de tarifas.

IOTA es el protocolo de software que se desarrolló como resultado del desarrollo de JINN, el título de trabajo para un nuevo tipo de microprocesador basado en métodos de cálculo ternario. Básicamente, esto significa que este procesador no maneja los estados binarios de 1 o 0, como lo hacen todos los procesadores en el mercado. Este nuevo sistema puede manejar los estados +1, 0 y -1.

Por el momento, cada computadora que quiera enviar una transacción en Tangle de IOTA debe calcular y confirmar otras dos transacciones antes, a través de la prueba de trabajo. Con JINN, esto se puede hacer en cualquier dispositivo sin tener una computadora encendida. Esto quiere decir que cada automóvil, teléfono móvil, refrigerador o cualquier dispositivo está habilitado para enviar transacciones sobre Tangle porque ahora puede hacer la prueba de trabajo necesaria.

JINN se anunció por primera vez en septiembre de 2014 en el foro NXT. NXT fue una de las primeras criptomonedas en abrir un Intercambio de activos descentralizado. En este intercambio, se podría comprar activos de varios tipos, entre los cuales también estaba el *token* JINN. Entonces, NXT Asset Exchange fue el lugar para obtener algo de dinero para financiar la idea de JINN.

NXT fue inventado por un desarrollador llamado Sergey Ivancheglo. Él es la figura clave en el desarrollo técnico y la realización de IOTA. Por esta razón

él se centró en la relación JINN / IOTA y ha sido un activo para todo el proyecto desde entonces.

6.3. Smart cities

Las ciudades inteligentes serán un gran tema en el futuro cercano. El negocio con ciudades inteligentes está en auge, se pronostica un crecimiento anual del 19 %, Se tiene la expectativa que el mercado global alcance un volumen de $ 800 mil millones para 2020. Las ciudades quieren reducir costos y aumentar la eficiencia, pero los aspectos ambientales y la optimización del tráfico también juegan un papel importante.

La ciudad de Las Vegas, por ejemplo, ha anunciado que invertirá aproximadamente $ 500 millones en infraestructura inteligente en los próximos años. Un distrito entero en el centro de la ciudad ha sido nombrado ‘distrito de innovación’. La optimización del tráfico basada en datos de tráfico en tiempo real y el establecimiento de un sistema de vehículo a infraestructura están destinados a hacer que los vehículos autónomos sean mucho más fáciles.

Actualmente, se está probando un autobús sin conductor que recibe señales de tráfico en tiempo real y las usa para determinar su velocidad.

En el área de San Francisco, hubo un proyecto de faros llamado baliza, ha ahorrado alrededor de $ 8 millones desde su lanzamiento al usar 5 000 luces inteligentes. Las balizas son una especie de balizas de radio inteligentes que se pueden abordar a través del estándar Bluetooth para que las luces solo se enciendan por la noche.

Mike Mansuetti, presidente de Bosch Norteamérica, menciona que los sensores Bosch son los ojos y oídos de la ciudad conectada. En este caso, su cerebro es el software. Además, se afirmó que para 2020 todos los productos electrónicos estarían habilitados para la web. Imaginablemente, esto dará como resultado una increíble cantidad de datos que se liberarán. Las capacidades de escalado y la velocidad de IOTA le permiten ser la base de todas estas transacciones de información.

6.4. Monitoreo del clima

La idea es aplicar IOTA para analizar la calidad del aire, la humedad y la concentración de polen para mejorar la calidad general mediante la implementación de medidas en caso de ser necesario. El producto para recopilar la información ya está funcionando y ha recibido el Premio a la Innovación CES 2018, es llamado The Climo. Este dispositivo mide el estado del aire y otros factores.

Varias de estas cajas Climo se implementaron en Las Vegas justo antes del CES para mostrar las capacidades a los asistentes a la conferencia.

La idea es recopilar datos de tantos puntos que el número total de fuentes de información evitará resultados sesgados. Además, también podría centrarse en un área específica de la ciudad para comparar los datos con otras partes de la ciudad.

6.5. Industria

Se están desarrollando aplicaciones IOTA para la industria del transporte, porque en los casos en que se debe rastrear la mercancía, el Tangle ofrece

muchas ventajas. Si bien en la industria del transporte todavía se hacen muchas cosas con papel, estos procesos se están volviendo cada vez más digitales. Además, del aspecto medioambiental, se puede mejorar la documentación, la comunicación y el flujo de pagos.

6.6. Amazon

Amazon en sí mismo es básicamente más grande que cualquier industria en este momento. Lo que decidan, otros lo seguirán. La actual directora de internet de las cosas en Amazon, Joanna Peña-Bickley, publicó a finales de 2017 una serie de tweets en favor de IOTA. Ella apoyó a IOTA y dijo que Amazon ahora lo está contemplando.

6.7. Otras aplicaciones

En el sector energía, muchas de las grandes plantas de energía probablemente tendrán más o menos solo una función de respaldo en el futuro. Un sinnúmero de pequeños sistemas eólicos y fotovoltaicos proporcionarán cada vez más la potencia necesaria, pero deben trabajar juntos de forma óptima y compartir sus datos entre ellos.

Esto hará que la transición energética sea el proyecto de TI más grande de todos los tiempos y solo tendrá éxito en combinación con la digitalización. Por lo tanto, los flujos de pago deben poder reenviarse de forma rápida y confiable en un sistema de este tipo con una gran transferencia de datos. En el futuro, millones de productores y consumidores deberán comunicarse en tiempo real, compartiendo no solo información sino también valores digitales.

En el sector salud, una de las medidas clave para el tratamiento exitoso de enfermedades crónicas es el monitoreo frecuente de los valores de salud más importantes de un paciente. El problema es que el aumento de visitas a los hospitales o centros de pruebas afectará la vida diaria del paciente y aumentará el costo del tratamiento.

Aquí es donde entran las soluciones de IoT. Un paciente con una enfermedad crónica podría estar equipado con múltiples dispositivos de IoT en red. IOTA tiene como objetivo permitir una mayor integridad de los datos dentro de la industria de la salud. Al transmitir y almacenar de manera segura los registros médicos individuales en el libro de contabilidad distribuido de IOTA, el acceso a los registros médicos privados puede ser confiable, seguro y controlado.

7. INVERSIÓN EN IOTA

7.1. Mercado de valores

El mercado de valores se refiere a los mercados públicos que existen para emitir, comprar y vender acciones que cotizan en una bolsa de valores. Las acciones representan la propiedad fraccional de una empresa. Un mercado de valores que funciona de manera eficiente se considera crítico para el desarrollo económico, ya que brinda a las empresas la capacidad de acceder rápidamente al capital del público.

El mercado de valores tiene un propósito muy importante, brindar a los inversores la oportunidad de compartir las ganancias de las empresas que se cotizan en la bolsa de valores. Los inversionistas pueden tomar ventaja de las compras de acciones de dos maneras: cobrar dividendos de manera regular o vendiendo las acciones que han comprado por una ganancia si el precio de las acciones ha subido desde su precio de compra.

7.2. Casas de cambio

Un cambio de moneda es un negocio que tiene el derecho legal de cambiar una moneda por otra a sus clientes. El cambio de divisas del dinero físico generalmente se realiza en un mostrador a través de un cajero. Las empresas de cambio de divisas que operan tales transacciones se pueden encontrar en una variedad de formas y lugares.

Puede ser una pequeña empresa independiente que opera desde una sola oficina, o puede ser una cadena más grande de pequeñas cabinas de servicios de cambio en los aeropuertos, también puede ser un gran banco internacional que ofrece servicios de cambio de divisas en sus cajeros.

Los servicios de cambio de divisas también se pueden encontrar a través de empresas que ofrecen estos servicios en línea. Esto se puede ofrecer como parte de los servicios prestados por un banco, corredor de divisas u otra institución financiera. Un negocio de cambio de divisas se beneficia de sus servicios ya sea ajustando el tipo de cambio o cobrando tarifas o ambos.

7.3. *Broker*

Un *broker* o corredor es una parte independiente, cuyos servicios se utilizan ampliamente en algunas industrias. La principal responsabilidad de un *broker* es facilitar como un intermediario, las operaciones entre vendedores y compradores.

Los corredores pueden proporcionar estudios de mercado y datos de mercado. Además, pueden representar al vendedor o al comprador, pero generalmente no a ambos al mismo tiempo. Los corredores son casi siempre necesarios para la compra y venta de instrumentos financieros, deben tener las herramientas y los recursos para llegar a la mayor base posible de compradores y vendedores.

Luego seleccionan a estos compradores o vendedores potenciales para encontrar la pareja perfecta. Otro beneficio de usar un corredor es el costo, pueden ser más baratos en mercados más pequeños con cuentas más pequeñas o con una línea limitada de productos.

7.4. Valor de IOTA en el mercado

El valor actual de IOTA en el mercado es de $ 0,27, esto es equivalente a Q 2,10 IOTA, es el 17º activo digital más grande con un valor de $ 745 millones en el mercado de las criptomonedas, se ha estado moviendo recientemente en un rango estrecho. La moneda ha perdido un 1,8 % de su valor en el día a día en medio de una venta global en el mercado de criptomonedas. IOTA se recuperó del reciente mínimo de $ 0,2400 tocado el 24 de septiembre; sin embargo, el impulso al alza se ha desvanecido.

El precio ha estado cotizando por encima desde que quebró al alza a finales de septiembre. Además, es probable que el precio siga una línea de soporte ascendente, que posiblemente podría tener una pendiente ligeramente diferente debido a la presencia significativa de mechas largas más bajas.

Figura 6. **Precio IOTA últimas 24 horas**

Fuente: *Precio IOTA*. https://www.coinbase.com/price/iota?locale=es. Consulta: 27 de octubre de 2019.

Figura 7. **Valor IOTA en los últimos dos años**

Fuente: *IOTA gráficos.* https://coinmarketcap.com/es/currencies/iota/. Consulta: 27 de octubre de 2019.

Alcanzó su punto máximo en diciembre de 2017 cuando empezó a darse a conocer la criptomoneda, llegó a un precio de $ 4,92. A partir de esa fecha, ha bajado su precio considerablemente hasta caer a menos de $ 1. Sin embargo, cuando la red de IOTA crezca inevitablemente, IOTA tendrá una gran demanda y será una criptomoneda muy rentable.

7.5. E-Wallet IOTA

El término billetera describe una cuenta en una criptomoneda respectiva, está asegurado con una contraseña. En IOTA se les llama semilla, en otras criptomonedas se les llama claves privadas. Las billeteras son el principal punto de acceso de las criptomonedas.

La billetera es muy parecida a un sello con el nombre de su propietario. En las criptomonedas, las transacciones se registran en el libro mayor y todos pueden registrar una nueva transacción con su sello. Luego, otros confirmarán que el sello es válido. El sello es un signo de autoridad para transferir monedas entre una billetera A y una billetera B.

Todos los participantes saben que este sello confirmó una transacción y pueden verificarlo. La billetera es básicamente la capacidad de sellar (finalizar) una transacción. Sellar una transacción es cuando ingresa su clave pública y privada o se inicia en IOTA.

El sello también es importante, porque si se pierde, ya no se puede acceder a la cuenta. La persona que encuentra este sello puede ejecutar nuevas transacciones desde esta cuenta. Entonces, la billetera es al principio una combinación simple de cadenas: la dirección de publicación a la que se envían las IOTA y la clave de acceso llamada semilla.

Las billeteras contienen su criptomoneda, no físicamente, pero la red acepta que esta dirección contenga una cierta cantidad de criptomonedas. Otras funciones de las billeteras son:

- Control de las claves privadas.
- Fácilmente utilizable.
- Comunidad de desarrolladores activos.
- Posibilidades de respaldo: muchas billeteras se pueden guardar en algún lugar o de alguna manera.
- Operabilidad en diferentes plataformas, por ejemplo, Windows, Mac, Linux, entre otros.

7.6. ¿Por qué invertir en IOTA?

Internet de las cosas ofrece la posibilidad de usar la plataforma en desarrollo para los proveedores de servicios de comunicación (CSP) con el fin de estudiar las nuevas posibilidades de crecimiento del sector y el aumento de ingresos. Para el 2020 se tiene como expectativa el crecimiento de las conexiones mediante IoT hasta un millón.

Según expertos, en los próximos diez años, el costo de la criptomoneda IOTA aumentará progresivamente debido a que combinará más de 50 mil millones de dispositivos.

IOTA ha atraído una tremenda atención positiva de los principales actores del mundo de la tecnología. Ha resistido tormentas y ha mantenido su valor. Hoy, IOTA tiene un valor de $ 1,93, lo que representa un aumento de 2,885 % de su precio anterior. Su valor está garantizado para seguir aumentando gracias a inversiones estratégicas y asociaciones.

7.7. Potencial de IOTA en el mercado

Al considerar las monedas en la comparación histórica, generalmente necesitaban algún tipo de autoridad central para mantener su valor y estabilidad. Temas como la regulación y la seguridad también se pueden garantizar más fácilmente. Sin embargo, las criptomonedas tienen un gran potencial porque estas reglas se representan en su código de programa. Son de código abierto y todos pueden verlo.

A diferencia de Bitcoin, IOTA tiene más potencial, debido a su caso de uso y construcción muy especial:

- Escalabilidad: mientras más usuarios ingresen a la red, más estable se convierte y se pueden confirmar más transacciones. Eso es exactamente lo contrario a Bitcoin, donde la red está congestionada.

- Creciente internet de las cosas: el IoT está simplemente en sus primeros pasos y será un factor para los próximos 50 años o más.

- Usuarios importantes: empresas como Bosch y Microsoft están probando IOTA.

- Euforia general en torno a las criptomonedas: si el precio sube o baja, el interés general sigue creciendo, también lo hace la demanda de esta clase de activos. También, surgen nuevas posibilidades de inversión.

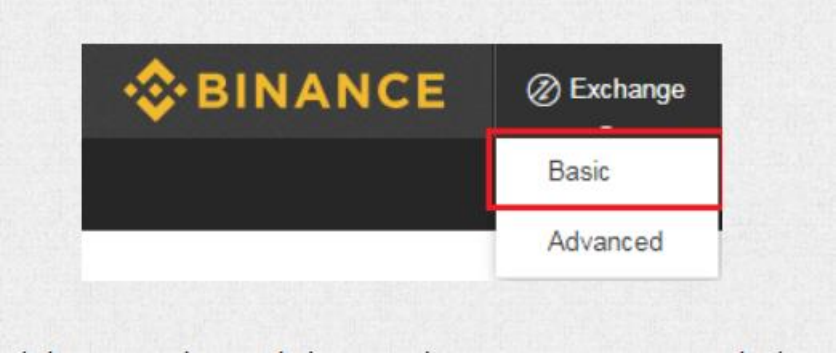
- Sin tarifas de transacción: esto es realmente muy importante.

7.8. ¿Cómo comprar IOTA?

Los pasos para comprar IOTA son:

- Registrarse https://www.binance.com/en/register?ref=10900506.
- Verificar cuenta a través del correo electrónico.
- Una vez verificada la dirección de correo electrónico, ir a depósitos y depositar bitcoins o ether.
- Para comprar IOTA se debe intercambiar por Bitcoin o ether. Una vez comprado fondos, estos se pueden intercambiar por IOTA. En la plataforma se elige Basic como en la figura 8.

Figura 8. **Plataforma Binance para comprar IOTA**



Fuente: *How to buy IOTA.* https://howtobuyiota.co.uk/#binance. Consulta: 27 de octubre de 2019.

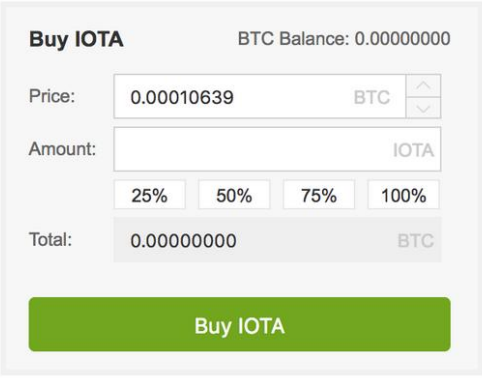
- Luego se debe encontrar elegir IOTA y elegir la moneda de cambio. Si se quiere comprar IOTA con Ethereum, escoger IOTA / ETH. Si es Bitcoin la moneda de cambio, estarías buscando IOTA / BTC.

Figura 9. **Elegir moneda de cambio**

Fuente: *How to buy IOTA.* https://howtobuyiota.co.uk/#binance. Consulta: 27 de octubre de 2019.

Completar con la cantidad de IOTA a comprar y elegir el botón ‘comprar IOTA’.

Figura 10. **Comprando IOTA**



Fuente: *How to buy IOTA.* https://howtobuyiota.co.uk/#binance. Consulta: 27 de octubre de 2019.

CONCLUSIONES

1. IOTA es uno de los proyectos más únicos en el espacio de las criptomonedas, considerando la creación del Tangle y el alto objetivo de convertirse en la moneda principal para el internet de las cosas. Además, el Tangle es beneficioso porque proporciona los medios para transacciones sin comisiones, es teóricamente resistente a los cuánticos y extremadamente escalable.

2. La red de IOTA tiene que crecer y madurar para convertir en un sistema de pago sólido, confiable y estable. Creo que esta tecnología nació con anticipación y en un futuro cercano, mostrará un crecimiento significativo. Dado que está ligado al internet de las cosas, esto hará que la red crezca inevitablemente, IOTA tendrá una gran demanda que hará que Tangle sea usada en muchos entornos y eleve la confianza de la criptomoneda.

3. Bitcoin mantendrá una ventaja y seguirá siendo la principal criptomoneda con la mayor capitalización de mercado durante mucho tiempo, simplemente porque es extremadamente popular, tanto entre los corredores, comerciantes y usuarios normales. El objetivo de las nuevas criptomonedas no es superar a Bitcoin, sino encontrar su propio uso y papel en la economía. IOTA es obviamente algo que encaja armoniosamente con esta economía, es un buen momento y comienzo para esta novedosa tecnología criptográfica. Por lo que la tarea fue mostrar IOTA como una alternativa.

4. IOTA es una moneda muy prometedora es la criptomoneda IoT número uno, probablemente seguirá siendo para el próximo año. Aún es una inversión rentable para mediano y largo plazo, ya que tiene buena base en IoT y se mantiene en el top 20 de criptomonedas. La impresión general del proyecto es buena, considerando el potencial de crecimiento y los aspectos negativos, es una posición considerable en la cartera de todos. Es importante recordar que no solo existe el enorme potencial de crecimiento, también, la tecnología está apostando por ser segura y confiable.

RECOMENDACIONES

1. Investigar otros casos de uso donde se puede utilizar IOTA, de esa manera se tendrá un aprendizaje amplio y se conocerá todas las ventajas que puede brindar IOTA.

2. Si se va a invertir en IOTA, revisar los blogs de criptomonedas; actualmente, se encuentran varios blogs en inglés y en español con información actualizada para revisar los movimientos y tendencias de la moneda. Además, de visualizar las alianzas que hace la Fundación IOTA con empresas de alto prestigio para crecer en el mercado.

3. Existen diversas plataformas para invertir en criptomonedas, recomiendo utilizar Binance, ya que es la más utilizada, es segura y es la más completa y maneja una amplia gama de criptomonedas.

BIBLIOGRAFÍA

1. HARDT, Marcus. *Avances de IOTA y la tecnología Tangle*. Traders Land. [en línea]. <https://traderslandfx.com/noticia/3908/>. [Consulta: 19 de octubre de 2019].

2. AGUIRRE, Jorge. *Curso de criptografía aplicada.* España: Creative Commons, 2018. 135 p.

3. BLANCO, David*. IOTA, conectando el mundo.* Tecnología para desarrollo. [en línea]. <https://www.paradigmadigital.com/dev/>. [Consulta: 01 de octubre de 2019].

4. GÓMEZ, Rafael*. Cómo minar bitcoin y otras criptomonedas*. [en línea]. <https://www.criptonoticias.com/criptopedia/como-minar-bitcoin-criptomonedas>. [Consulta: 12 de octubre de 2019].

5. DUNCAN, Sean. *Cryptocurrency Investing and Trading in the Blockchain. Bitcoin, Ethereum, Litecoin, IOTA, Ripple, Dash, Monero, Neo & More!* Estados Unidos: Cascade Publishing, 2018. 52 p.

6. HERRERA, Carlos. *El funcionamiento de IOTA*. Qué es IOTA. [en línea]. <https://www.queesiota.info/como-funciona-iota/>. [Consulta: 30 de septiembre de 2019].

7. PÉREZ, Otto*. El origen de las criptomonedas*. Revista Muy Interesante. [en línea]. <https://www.muyinteresante.com.mx/ciencia-y-tecnologia/el-origen-de-las-criptomonedas/>. [Consulta: 27 de septiembre de 2019].

8. CABALLERO, Daniela*. Estudio del comportamiento de criptomonedas con un crecimiento orgánico producto de un sistema pump & dump*. [en línea]. <https://docplayer.es/amp/152653971-Estudio-del-comportamiento-de-criptomonedas-con-un-crecimientos-organicos-y-espurios-producto-de-un-sistema-pump-dump.html>. [Consulta: 27 de septiembre de 2019].

9. FANHLE, Pablo. *Estudio del comportamiento de criptomonedas con un crecimientos orgánicos y espurios producto de un sistema pump & dump.* Trabajo de graduación de Magister en Dirección Estratégica y Tecnológica. Instituto Tecnológico de Buenos Aires, 2019. 156 p.

10. FANJUL, Sergio*. Todo lo que los sensores pueden hacer por ti.* Talento digital. [en línea]. <https://elpais.com//2016//07/14811.html>. [Consulta: 20 de octubre de 2019].

11. GÓMEZ, Iván*. Tiemblan las criptomonedas, computación cuántica es capaz de romper algoritmos de encriptación.* Criptonoticias. [en línea]. <https://www.criptonoticias.com/seguridad/tiemblan-criptomonedas-computacion-cuantica-romper-algoritmos-encriptacion/>. [Consulta: 10 de octubre de 2019].

12. GÓNZALEZ SÁNCHEZ, Javier. *Introducción al modelo de servicios distribuidos con IOTA.* Trabajo de graduación de Máster Universitario en Seguridad de las Tecnologías de la información y de las comunicaciones. Universitat Oberta de Catalunya, 2018. 50 p.

13. GUTIÉRREZ, Juan. *IOTA pierde terreno con relación al dólar*. GuiaBitcoin. [en línea]. <https://guiabitcoin.com/news/iota-pierde-terreno-con-relacion-al-dolar>. [Consulta: 25 de octubre de 2019].

14. HOUBEN, Robby, SNYERS, Alexander. *Cryptocurrencies and blockchain.* Bélgica: European Parliament, 2018. 103 p.

15. *How to buy IOTA on Binance*. Binance. [en línea]. <https://howtobuyiota.co.uk/#binance>. [Consulta: 27 de octubre de 2019].

16. IGLESIAS, Andreina*. La computación cuántica podría hacer vulnerable a la Blockchain.* Bitcoin.es. [en línea]. <https://bitcoin.es/actualidad/la-computacion-cuantica-podria-hacer-vulnerable-a-la-blockchain/>. [Consulta: 09 de octubre de 2019].

17. *IOTA*. Coinbase. [en línea]. <https://www.coinbase.com/price/iota?locale=es>. [Consulta: 24 de octubre de 2019].

18. *IOTA*. CoinMarketCap. [en línea]. <https://coinmarketcap.com/es/currencies/iota/>. [Consulta: 24 de octubre de 2019].

19. *Iota, la criptomoneda del futuro*. Vigilante inversores. [en línea]. <https://vigilanteinversores.com/iota/>. [Consulta: 29 de septiembre de 2019].

20. MANUEL, Juan*. IOTA, una criptomoneda para el internet de las cosas.* IOTA Futura. [en línea]. <https://iotfutura.com/arquitecturas-iot/iota-the-tangle#Resistencia_a_la_computacion_cuantica>. [Consulta: 08 de octubre de 2019].

21. MARTÍ, Montse. *Seguridad en el Internet de las cosas. Estudio de IOTA para el Internet of Things.* Trabajo de graduación de Máster Universitario en Seguridad de las Tecnologías de la información y de las comunicaciones. Universitat Oberta de Catalunya, 2018. 69 p.

22. MORENO, Bibiana; SOTO, Francely; VALENCIA, Nancy; SÁNCHEZ, Adelina. *Criptomonedas como alternativa de inversión, riesgos, regulación y posibilidad de monetización en Colombia.* Trabajo de graduación de Especialización Gerencia Financiera. Universidad de Bogotá Jorge Tadeo Lozano. Facultad Ciencias Económicas y Administrativas, 2018. 50 p.

23. MUELLER, Chris*. The origins of Jinn and IOTA* Hello IOTA. [en línea]. <https://helloiota.com/origins-of-jinn-and-iota/>. [Consulta: 20 de octubre de 2019].

24. OLIVARES, José Luis*. Un ordenador cuántico supera los esquemas de encriptación.* Ciencia Plus. [en línea]. <https://iotfutura.com/arquitecturas-iot/iota-the-tangle#Resistencia_a_la_computacion_cuantica>. [Consulta: 09 de octubre de 2019].

25. POPOV, Serguei. *The Tangle.* Rusia: Amazon, 2018. 28 p.

26. ROMAN, Alexander. *IOTA Introduction to the Tangle Technology.* Estados Unidos: Crypto Pay, 2018. 88 p.

27. SOORYA, Rohit. *Cryptocurrency Guide for beginners.* Estados Unidos: Amazon, 2018. 83 p.

28. TAHIRI, Valdrin*. IOTA tiene un gran potencial para un movimiento ascendente, afirma un trader*. Beincrypto. [en línea]. <https://es.beincrypto.com/iota-tiene-un-gran-potencial-para-un-movimiento-ascendente-afirma-un-trader>. [Consulta: 27 de octubre de 2019].

29. HUERTA, Jesús. *Todo sobre criptomoneda IOTA*. Cripto Minería. [en línea]. <https://cripto-mineria.com/criptomonedas/iota>. [Consulta: 24 de octubre de 2019].

30. KOLBL, Stefan. *Troika, a ternary hash function*. Cybercript. [en línea]. <https://www.cyber-crypt.com/troika/>. [Consulta: 10 de octubre de 2019].

APÉNDICES

Apéndice 1. **Programando Hola Mundo con IOTA, clase Index.js**

```
$(document).ready(function() {

    var iota = new IOTA({
        'host': 'http://localhost/holaMundo',
        'port': 8086
    });

    var posicion;
    var direccion;
    var contador = 0;

    function toggleSidebar() {
        $(".button").toggleClass("active");
        $("main").toggleClass("move-to-left");
        $(".sidebar-item").toggleClass("active");
        $(".sidebar").toggleClass("donotdisplay");
    }

    function setPosicion(value) {

        posicion = "";
        value = value.toUpperCase();

        for (var i = 0; i < value.length; i++) {
            if (("9ABCDEFGHIJKLMNOPQRSTUVWXYZ").indexOf(value.charAt(i)) < 0) {
                posicion += "9";
            } else {
                posicion += value.charAt(i);
            }
        }
    }
```

Continuación del apéndice 1.

```
function getInfoCuenta() {

    iota.api.getAccountData(posicion, function(e, accountData) {
        console.log("Información cuenta: ", accountData);
        if (!direccion && accountData.direcciones[0]) {
            direccion = iota.utils.addChecksum(accountData.direcciones[accountData.direcciones.length - 1]);
            actualizarDireccionHTML(direccion);
        }

        var listaTransferencia = [];

        if (accountData.transfers.length > contador) {
            console.log("Recibido nuevo mensaje");
            accountData.transfers.forEach(function(transfer) {
                try {
                    var mensaje = iota.utils.extractJson(transfer);
                    console.log("Json extraído de la transacción: ", mensaje);

                    mensaje = JSON.parse(mensaje);
                    console.log("JSON: ", mensaje);

                    var nuevoTexto = {
                        'name': mensaje.name,
                        'mensaje': mensaje.mensaje,
                        'value': transfer[0].value
                    }
                    listaTransferencia.push(nuevoTexto);

                } catch(e) {
                    console.log("Transacción no contiene información en el JSON");
                }
            })
```

```
            })
            contador = accountData.transfers.length;
        }

        if (listaTransferencia.length > 0) {
            updateLeaderboardHTML(listaTransferencia);
        }
    })
}

$(".button").on("click tap", function() {
    toggleSidebar();
});

$("#posicionSubmit").on("click", function() {

    setPosicion($("#userposicion").val());
    $("#enterposicion").html('<div class="alert alert-success" role="alert">Guardado exitosamente. Puedes generar un mensaje.</div>');
    getInfoCuenta();
    setInterval(getInfoCuenta, 90000);
});

$("#gendireccion").on("click", function() {

    if (!posicion) {
        console.log("You did not enter your posicion yet");
        return
    }
    iota.api.getNewdireccion( posicion, { 'checksum': true }, function( e, direccion ) {

        if (!e) {
```

Continuación del apéndice 1.

```
            if (!e) {

                direccion = direccion;
                actualizarDireccionHTML(direccion);

            } else {

                console.log(e);
            }
        })
    })
});
```

Fuente: elaboración propia.

Apéndice 2. **Programando Hola Mundo con IOTA, clase send.js**

```
$(document).ready(function() {

    var iota = new IOTA({
        'host': 'http://localhost/holaMundo',
        'port': 8086
    });

    var posicion;
    var balance = 0;
    var direccion;

    function toggleSidebar() {
        $(".button").toggleClass("active");
        $("main").toggleClass("move-to-left");
        $(".sidebar-item").toggleClass("active");
        $(".sidebar").toggleClass("donotdisplay");
    }

    function setPosicion(value) {

        posicion = "";
        value = value.toUpperCase();
        for (var i = 0; i < value.length; i++) {
            if (("9ABCDEFGHIJKLMNOPQRSTUVWXYZ").indexOf(value.charAt(i)) < 0) {
                posicion += "9";
            } else {
                posicion += value.charAt(i);
            }
        }
    }
```

Continuación del apéndice 2.

```
function getInfoCuenta() {

    iota.api.getAccountData(posicion, function(e, accountData) {
        console.log("Información cuenta: ", accountData);

        if (!direccion && accountData.direcciones[0]) {
            direccion = iota.utils.addChecksum(accountData.direcciones[accountData.direcciones.length - 1]);
            actualizarDireccionHTML(direccion);
        }

        balance = accountData.balance;
        actualizarBalanceHTML(balance);
    })
}

function gendireccion() {

    console.log("Generando una dirección");
    iota.api.getNewdireccion(posicion, {'checksum': true}, function(e,direccion) {
        if (!e) {
            console.log("Nueva dirección generada: ", direccion)
            direccion = direccion;
            actualizarDireccionHTML(direccion)
        }
    })
}
```

```
function enviarTransferencia(direccion, value, messageTrytes) {

    var transfer = [{
        'direccion': direccion,
        'value': parseInt(value),
        'message': messageTrytes
    }]

    console.log("Enviando transferencia", transfer);

    iota.api.enviarTransferencia(posicion, 3, 8, transfer, function(e) {

        if (e){

            var html = '<div class="alert alert-danger alert-dismissible" role="alert"><button type="button" class="close" d
            $("#send__success").html(JSON.stringify());

            $("#submit").toggleClass("disabled");

            $("#send__waiting").css("display", "none");

        } else {

            var html = '<div class="alert alert-info alert-dismissible" role="alert"><button type="button" class="close" dat
            $("#send__success").html(html);

            $("#submit").toggleClass("disabled");

            $("#send__waiting").css("display", "none");

            balance = balance - value;
```

Continuación del apéndice 2.

```
            balance = balance - value;
            actualizarBalanceHTML(balance);
        }
    })
}

$(".button").on("click tap", function() {
    toggleSidebar();
});

$("#posicionSubmit").on("click", function() {
    setPosicion($("#userposicion").val());
    $("#enterposicion").html('<div class="alert alert-success" role="alert">Guardado exitosamente. Puedes generar una tra
    getInfoCuenta();
    setInterval(getInfoCuenta, 90000);
});

$("#gendireccion").on("click", function() {
    if (!posicion)
        return

    gendireccion();
})

$("#submit").on("click", function() {

    if (!posicion) {
        var html = '<div class="alert alert-warning alert-dismissible" role="alert"><button type="button" class="close" d
        $("#send__success").html(html);
        return
    }
```

```
    if (!balance || balance === 0) {
        var html = '<div class="alert alert-warning alert-dismissible" role="alert"><button type="button" c
        $("#send__success").html(html);
        return
    }

    var name = $("#name").val();
    var value = parseInt($("#value").val());
    var direccion = $("#direccion").val();
    var message = $("#message").val();

    if (!name || !value || !message)
        return

    if (value > balance) {
        var html = '<div class="alert alert-warning alert-dismissible" role="alert"><button type="button" c
        $("#send__success").html(html);
        return
    }

    var messageToSend = {
        'name': 'Jeff',
        'message': 'Hola Mundo'
    }

    try {
        console.log("Enviando mensaje: ", messageToSend);
        var mensajesTernarios = iota.utils.toTrytes(JSON.stringify(messageToSend));
        console.log("Convirtiendo el mensaje en ternario: ", mensajesTernarios);
```

Continuación del apéndice 2.

```
            $("#send__waiting").css("display", "block");
            $("#submit").toggleClass("disabled");
            $("#send__success").html();
            enviarTransferencia(direccion, value, mensajesTernarios);

        } catch (e) {

            console.log(e);
            var html = '<div class="alert alert-warning alert-dismissible" role="alert"><button type="button" c
            $("#send__success").html(html);

        }
    })
});
```

Fuente: elaboración propia.