FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

Estudio de la Tecnología Blockchain para el Aseguramiento de los Dispositivos IoT

AUTOR

Estefano Alejandro Rodríguez Espinoza

AÑO

2020

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

ESTUDIO DE LA TECNOLOGÍA BLOCKCHAIN PARA EL ASEGURAMIENTO DE LOS DISPOSITIVOS IOT

Trabajo de Titulación presentado en conformidad con los requisitos establecidos para optar por el título de Ingeniero en Electrónica y Redes de Información.

Profesor Guía

William Villegas

Autor

Estefano Alejandro Rodríguez Espinoza

Año 2020

DECLARACIÓN PROFESOR GUÍA

"Declaro haber dirigido el trabajo, Estudio de la Tecnología Blockchain para el Aseguramiento de los Dispositivos IoT, a través de reuniones periódicas con el estudiante Estefano Alejandro Rodríguez Espinoza, en el semestre 202020, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación".

William Eduardo Villegas Chiliquinga

PhD. En Informática

C.I: 1715338263

DECLARACIÓN PROFESOR CORRECTOR

"Declaro haber revisado este trabajo, Estudio de la Tecnología Blockchain para el Aseguramiento de los Dispositivos IoT, del estudiante Estefano Alejandro Rodríguez Espinoza en el semestre 202020, dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación".

Luis Santiago Criollo Caizaguano

Máster en Redes de Comunicaciones

C.I: 1717112955

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

"Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes".

Estefano Alejandro Rodríguez Espinoza

C. I: 1725869836

AGRADECIMIENTOS

Agradezco a mis padres por darme la oportunidad de continuar mis estudios, además de a mis profesores que fueron los guías durante mi vida universitaria y a mis compañeros quienes estuvieron apoyándome continuamente.

RESUMEN

Hoy en día cuando se escucha del término Blockchain suele asociarse con lo que son los bitcoins y otros tipos de criptomonedas semejantes. Sin embargo, este no es el único uso que se le da a este tipo de tecnología que tuvo su auge en el año 1991 por Stuart Habel y W. Scott. Este tipo de tecnología ha brindado seguridad en diferentes tipos de mercados, como pueden ser instituciones financieras o incluso dentro de lo que es IoT.

En el siguiente trabajo de titulación se busca como objetivo principal el brindar opciones para asegurar los dispositivos IoT aprovechando las características y posibilidades que posee dicha tecnología. Desde un inicio este tipo de seguridad a manera de una cadena de bloques que fuera asegurada de manera criptográfica no fue muy denotada hasta la aparición del bitcoin, sin embargo, en la actualidad se espera el crecimiento y uso de esta debido a la seguridad que esta puede brindar a los usuarios finales. Logrando así almacenar registros únicos, consensuados y distribuir estos datos en distintas partes de la red protegiendo y asegurando la disponibilidad de los datos que se están transmitiendo.

Para poder brindar las posibles soluciones para poder implementar en algún otro proyecto a seguir se realizará un estudio del funcionamiento y características tanto de IoT como del Blockchain, teniendo así en claro escenarios realistas en el cual este tipo de encriptación pueda ser funcional.

Dando como resultados algunos modelos funcionales y aplicables para una transmisión segura de los dispositivos IoT dando paso a futuras aplicaciones de estos. Finalmente, se realizará un análisis de los resultados obtenidos para poder evidenciar el cumplimiento del objetivo principal que se plantea para este trabajo de titulación.

ABSTRACT

Today when you hear about the term Blockchain it is often associated with what bitcoins and other similar types of cryptocurrencies are. However, this is not the only use given to this type of technology that had its rise in 1991 by Stuart Habel and W. Scott. This type of technology has provided security in different types of markets, such as financial institutions or even within what is IoT.

In the following degree work, the main objective is to provide options to secure IoT devices taking advantage of the characteristics and possibilities that this technology has. From the beginning, this type of security in the form of a Blockchain that was cryptographically secured was not highly denoted until the appearance of bitcoin, however, its growth and use is currently expected due to the security that this can provide to end users. Getting in this way, storing unique, agreed data records and distributing these in different parts of the network, protecting and ensuring the availability of the data being transmitted.

In order to provide possible solutions to implement in some other project to follow, a study of the operation and characteristics of both IoT and Blockchain will be carried out, getting a clear realistic situation in which, this type of encryption can be functional.

Resulting in some functional and applicable models for a secure transmission of IoT devices, giving way to future applications for these. Finally, an analysis of the results obtained will be carried out in order to demonstrate the fulfillment of the main objective that is proposed for this degree work.

ÍNDICE

1. INTRODUCCIÓN

En la actualidad el uso de la tecnología Blockchain ha ido incrementando en diferentes campos y mercados. A pesar de que se trata a la par el tema de las criptomonedas cuando se habla de Blockchain es muy importante mencionar que este solo sería una parte muy pequeña de lo que puede englobar toda esta tecnología. (ESET, 2018).

Sin embargo, es necesario tener en cuenta que la primera aparición de esta tecnología fue gracias a la ayuda de los bitcoins, la cual a diferencia de las monedas fíat no poseían un banco central que las controlase, sino eran todo lo contrario el cual llevaba su control miles de dispositivos que estaban distribuidos alrededor de todo el mundo, permitiendo que cualquier tipo de persona pudiera ser partícipe de este tipo de ecosistema únicamente con la descarga de un software el cual era de código abierto. (Binance, 2017).

En este caso el Blockchain fue utilizado como si fuera un libro contable al momento de tratar y con los datos solo podían agregarse al final para no modificar el resto de la cadena, dando como resultado una cadena de datos extremadamente complicada de ser atacada por terceros incluyendo un hash o puntero bloqueando las modificaciones o eliminaciones de la información y en el caso de ser intervenida dicha información muestra el problema y se corta el paso de esta información al dar errores al tratar de pasar el nuevo hash creado. (Binance, 2017).

Este tipo de seguridad llamada hash era principalmente utilizada para crear una huella única de ese bloque de datos para enviarlo al siguiente, asegurando el bloque incluso al más mínimo cambio que se realice, dando una identidad única a cada parte de la cadena, sin la posibilidad de dejar aperturas o vulnerabilidades haciendo que la tecnología Blockchain aplicada en este tema sea completamente segura. A pesar de que sea un método seguro para este tipo de transacciones no en todos los países es permitido el Bitcoin o criptomonedas principalmente definido por los gobiernos.

Otro tipo de aplicación en la cual puede ser aplicada esta tecnología es dentro de los dispositivos IoT los cuales están incrementando exponencialmente su

aparición debido a las facilidades que estos equipos pueden brindar a un usuario final, pero con ello también aparecen nuevas vulnerabilidades debido a que no existen las suficientes normas para proteger la información que se pueden transmitir con estos dispositivos.

En cuanto a este tipo de dispositivos tecnológicos es posible definirlos como una agrupación o interconexión de equipos que pueden ser visibles en una red privada, dando la posibilidad a que estos puedan interactuar y compartir información. Teniendo en cuenta el avance tecnológico cualquier tipo de objeto hoy en día puede ser un dispositivo IoT, sin la necesidad de que un humano intervenga durante el proceso de comunicación por medio del internet o también conocido como una interacción M2M o maquina a máquina. (Deloitte, 2020).

Actualmente se tienen diferentes aplicaciones para esta tecnología buscando aplicar las ventajas, como pueden ser en entornos financieros o incluso con la creación de nuevas criptomonedas.

Para lo cual en el presente trabajo de titulación se realizara un estudio exhaustivo de las características de IoT y de Blockchain para así poder saber cuándo puede ser optimo combinar ambas tecnologías y sacar provecho a las funciones que brinda este tipo de seguridad para evitar el robo o perdida de la información, debido a que estos dispositivos van de la mano a las nuevas redes que se vienen como puede ser la red 5G, para poder mejorar el funcionamiento que estos pueden brindar al usuario final o en otro caso que le sirva dicha información para que el creador de un dispositivo en específico recolecte recomendaciones y datos para mejorar dicho producto, con la seguridad de que la información personal del usuario dueño del dispositivo no se malinterprete o modifique para el uso de terceros.

1.1 Alcance

El siguiente trabajo de titulación se basará en el estudio para la utilización de la tecnología Blockchain dentro de los dispositivos IoT, el cual buscará obtener datos sobre la viabilidad de esto a su vez que brindar un método innovador para dichas tecnologías emergentes.

Para realizar el tema antes mencionado se realizará inicialmente un análisis del funcionamiento de los dispositivos IoT y Blockchain logrando así obtener datos relevantes que darán paso a buscar una solución óptima para el entrelazamiento de los dos, facilitando y asegurando el uso de dichos dispositivos en la actualidad, mediante el uso de un modelo para la categorización de los diferentes aspectos de Blockchain.

1.2 Justificación

Debido al avance de la tecnología y la búsqueda de la implementación del 5G han incrementado enormemente los dispositivos IoT y con ello la inseguridad de los datos que se tiene al ser equipos que recopilan datos constantemente para su funcionamiento óptimo, por lo cual surge la necesidad de implementar tecnologías de encriptación para asegurar los datos enviados y lograr así salvaguardar la información de las personas.

Por lo tanto, salen a flote las distintas posibilidades y nuevas tecnologías día a día para tener una garantía solida al momento de transmitir los datos, entre ellas se hace presente Blockchain el cual busca ser un sistema prácticamente infalible e innovador para las tecnologías actuales.

En la actualidad la tecnología ha avanzado a un nivel exponencial entre ellos los dispositivos que buscan facilitar la vida diaria del ser humano e incluso almacenar algunos datos ayudando a los mismos, sin embargo, con ello también han aparecido diferentes vulnerabilidades de estos datos los cuales a pesar de que no se de mucha importancia a lo mismo pueden llegar a afectar a la integridad de las personas debido a que muchos de estos dispositivos IoT son capaces de recolectar datos sin el consentimiento de los usuarios y de manera

constante, por lo cual a su vez que aparecen estos dispositivos se buscan aplicar normas o reglamentos con los cuales estos deben manejarse, pero el avance de ellos dejan muchas fugas los cuales las personas malintencionadas buscan aprovecharse, para ello se plantea este proyecto al buscar una manera de asegurar los datos que se envían dentro de estos dispositivos y dar a conocer una solución para estas vulnerabilidades.

1.3 Objetivo General

Analizar las tecnologías Blockchain para el aseguramiento de los dispositivos IoT.

1.4 Objetivos Específicos

- Analizar el comportamiento e interacción que tienen los dispositivos IoT para denotar los puntos débiles de estas tecnologías.
- Realizar un estudio del cifrado Blockchain para comprender las capacidades que tiene esta tecnología.
- Categorizar los modelos de Blockchain existentes que se ajustan a las necesidades del internet de las cosas.

2. MARCO TEÓRICO

A continuación, dentro de este capítulo se detallarán los datos que corresponden tanto para los dispositivos IoT y a la tecnología Blockchain para poder comprender el funcionamiento que tienen ambas y la manera en la cual se pueden entrelazar para asegurar dichos dispositivos y salvaguardar la información que recolectan.

2.1 Introducción IoT

Para poder iniciar con el proyecto de investigación es necesario conocer los equipos a los cuales se busca implementar un método de aseguramiento de la información. Por lo cual podemos denotar que con el avance tecnológico estos dispositivos han sido mencionados con más frecuencia debido a las facilidades y beneficios que pueden brindar a la vida cotidiana de una persona, sin embargo, este es solo un tipo de punto de vista al darnos cuenta de que este tipo de equipos ya poseen una importancia tanto social, técnica o incluso económica dentro de la sociedad.

Hoy en día podemos encontrarlos ya aplicados dentro de diferentes áreas de empresas o incluso en nuestro propio hogar, ya sea combinados dentro de bienes de consumo, automóviles, electrodomésticos, servicios públicos, entre otros que dispongan de una conexión a internet y con la posibilidad de analizar datos en tiempo real para poder ser transformado en información útil, transformando todo el entorno en el que vivimos y hemos estado acostumbrados.

A su vez también se espera que el impacto de este tipo de dispositivos ya sea dentro del internet y en la economía crezcan exponencialmente e incluso según algunos expertos anticiparían que para el año 2025 ya existan alrededor de cien mil millones de equipos vinculados a lo que es el tema de IoT imponiendo un impacto enorme en lo económico. (Internet Society, 2015).

A pesar de que se mencione que traerán grandes beneficios este tipo de tecnología también vendrá de la mano con grandes desafíos los cuales se interpondrán a ellos, los cuales pueden incluir las herramientas de políticas y los

programas que se utilizan en la actualidad, englobando con ellos problemas con estándares o modelos de negocios, la vigilancia de estos dispositivos, la aceptación de estos y cambiar prácticamente todos los paradigmas con los cuales nos hemos mantenido tras generaciones. (Kranenburg, 2012).

Pero al mencionar todos estos cambios con los que vivimos cada día cada persona tendrá un punto de vista diferente del término IoT, llegado incluso a ser rechazado al momento de querer implementarlo si no se explica correctamente el funcionamiento o uso al cual se dará a un dispositivo normal y corriente con un acceso al internet, con la tecnología avanzando continuamente es posible decir que prácticamente cualquier dispositivo físico en el mundo puede llegar a ser como una computadora con acceso al internet. (UIT, 2005). Sin embargo, aunque se mencionen este tipo de frases no necesariamente significa que todos los dispositivos son una computadora como tal, sino que se busca dar comportamientos similares a estos equipos dando como tal la opción de ser reconocidas como minicomputadoras.

Por otro lado, hay personas las cuales consideran que son equipos inteligentes debido a la posibilidad que tienen de brindar datos útiles a una persona en específico en comparación con otro tipo de cosas las cuales vemos día a día. Dando como resultado una duda que nos puede surgir al intentar comprender desde que momento un objeto es comprendido por el termino de IoT, como puede ser un ejemplo muy básico, en el cual un alimento en específico contiene un código de barras, dentro de lo mencionado también podría entrar dentro del campo IoT, sin embargo, este tipo de información no se transmite de manera autónoma llegando a considerarse más como un estado, los cuales buscan principalmente comunicar algún tipo de información en específico con la ayuda de un tercero. (Meyer, 2009).

En un inicio el termino apareció por medio de Kevin Ashton alrededor de los años 1999, pero este término no fue generalizado como tal hasta tiempo después con la ayuda de Auto-ID Center el cual es un grupo de trabajo que busca la identificación de radiofrecuencias dentro de una red (RFID) a la par que otro tipo de tecnologías que refieren a la detección. (Auto-ID Labs, 2012).

Pero la definición de IoT no se mencionó dentro de ese tiempo, a pesar de haber existido un acuerdo que trababa de manera general a este término el cual identificaba que tenía que ver con el entrelazamiento de los objetos y una conectividad entre ellos.

Luego de una década se comenzó a buscar la manera para explicar que era como tal el internet de las cosas, pero no existía una definición única o universal en la cual se la pueda conocer a este tipo de tecnología, sin embargo, podemos referirnos a ella cuando dentro de un mismo escenario entrelazamos varios objetos, sensores o incluso artículos que vemos día a día en el entorno con lo que es la conectividad dentro de una red de datos.

Dando la posibilidad de que estos objetos mencionados con anterioridad puedan tener la capacidad de generar, intercambiar y utilizar información con la más mínima intervención de una persona o usuario. (Internet Society, 2015).

A pesar de que la búsqueda de lograr combinar todo tipo de objetos con la ayuda de redes para poderlos controlar y revisar sin encontrarse cerca de ellos ha existido durante varios años, recientemente con la influencia del mercado tecnológico como tal ha brindado la posibilidad de que estos pensamientos que iniciaron como un sueño se encuentre cada vez más cerca de la realidad. Esto principalmente a las mejoras que se le han dado al protocolo IP y los beneficios que estos pueden brindar para la transmisión de datos, dispositivos con tamaños prácticamente imperceptibles, prestación de servicios basados en la nube a la vez que equipamiento similar a hardware a un menor costo, dando una oportunidad a empresas emprendedoras de actualizar sus dispositivos y mejorar la eficiencia que posean en el momento.

Pero ya al momento de querer implementar como tal internet de las cosas en un campo en específico es necesario tener en cuenta que existen algunos modelos para poder controlar y monitorizar los dispositivos conectados, teniendo en cuenta que según cual se escoja se necesitaran manejar algunas características en específico.

Los principales modelos para la conectividad y aplicación de IoT pueden ser los siguientes:

- Dispositivo a Dispositivo
- Dispositivo hacia la nube
- Dispositivo hacia la puerta de enlace (gateway)
- Intercambio de los datos por medio del back-end

Estos tipos de modelos buscan buscar una flexibilidad al momento de brindar conexión entre los dispositivos que se utilizaran de IoT a su vez que mostrar maneras de conexión para poder brindar un valor agregado al usuario que desea implementar este tipo de tecnología. (Internet Society, 2015).

Las cuales se explicarán con mayor detalle en los siguientes puntos para saber cuál es el modelo más optimo en el caso de utilizar Blockchain.

A pesar de que no se desee implementar IoT o que las empresas busquen como tal ignorar dicha tecnología es necesario tener en cuenta que este tipo de tendencias tecnológicas absorberán los mercados y mientras más sencillo sea la manipulación y observación de equipos será un ahorro económico para tener en cuenta, por lo cual a pesar de las discrepancias de pensamiento que se presenten será necesario acoplarse a esta realidad para no ser apartados por el avance tecnológico continuo.

Esto afectara directamente a los proveedores de servicios, ya que al tener una mayor cantidad de dispositivos conectados a una misma red será necesario brindar una mejor calidad de servicio con un ancho de banda más grande para así no tener perdida de información ni problemas con la seguridad, por lo cual la aparición de la red 5G puede ser una gran solución a esta problemática y con ello llegar a tener un mundo completamente interconectado, eliminando limitaciones al momento de requerir algún servicio debido a que todo estará al alcance con una conexión a internet.

Dentro de lo que engloba IoT se pueden revisar varios campos para el estudio de esta tecnología, pero para este tipo de investigación se revisaran aquellos que puedan tener relación con la seguridad de los datos debido a que será la tecnología Blockchain la cual se utilizará en conjunto con IoT para asegurar que los datos que se envían no sean modificados ni utilizados para otro tipo de propósito. Para lo cual se analizará:

- Seguridad
- Privacidad
- Interoperabilidad
- Estándares

2.1.1 Seguridad

Un punto de increíble importancia de estos tipos de dispositivos es garantizar la seguridad, la confiabilidad de los datos y la estabilidad de las aplicaciones o servicios que ofrecen dentro de los equipos IoT, este es un tema de suma importancia para poder crear un ambiente de confianza con respecto a estos dispositivos y el uso que se les da conectados al internet. Esto es relevante debido a que al ser partícipes como usuarios del internet es necesario tener un grado alto de confianza con respecto a que dispositivos que son permitidos por la red y si estos son lo suficientemente seguros para poder recolectar y transmitir la información que se transmite por la misma, además de plantear un nivel de tolerancia para los riesgos que pueden llevar este tipo de actividades.

Ya en este punto el internet de las cosas no es muy distinto y lo que busca principalmente la seguridad enfocada para estos dispositivos esta principalmente dirigida a la capacidad que puede soportar y confiar un entorno en base a los usuarios. Este impacto es tal que, si los usuarios que dispongan de una red de internet no tienen la suficiente confianza de que la información que estos tipos de dispositivos tengan frente al mal uso o a daño de los datos, se provocaría una pérdida o renuncia al uso de estos tipos de equipos dentro de su red. Se puede decir que estos dispositivos pueden llegar a tener consecuencias globales para lo que es el comercio electrónico, las innovaciones técnicas que tengan, la

libertad de expresión de los usuarios e incluso llegar a englobar otros tipos de actividades que se realizan en línea. (Internet Society, 2015). Por lo cual los sectores que deseen aplicar este tipo de dispositivos como mejoras deben tener en consideración el tema de la seguridad que se aplicará como una de sus principales prioridades.

Como se sabe mientras más equipos o dispositivos tengamos conectados dentro de una red, aparecen nuevas maneras en las que terceros puedan buscar potenciales vulnerabilidades referentes a las seguridades que dispongan estos. Por tanto, los dispositivos dentro de la rama de IoT que no tengan implementada una correcta seguridad pueden llegar a ser fuentes de ciberataques, permitiendo que terceros que busquen perjudicar estos equipos realicen modificaciones y busquen sacar provecho de la información que estos obtengan.

Los dispositivos de IoT que no tengan un correcto funcionamiento o incluso que puedan estar mal diseñados llegarían a tener fugas las cuales permitan el robo de datos de los usuarios, dejando como tales flujos de información que pueden llegar a ser vitales a merced de personas malintencionadas, incluso dispositivos que ya no se utilicen o estén dañados pueden dejar puertas traseras abiertas para realizar ciberataques. Sin embargo, estos problemas se presentan principalmente en los equipos de IoT que se mencionan como baratos dentro de las redes de venta, que por lo general no poseen un sistema de seguridad que corrobore su funcionamiento. Esto llega a ser cada vez más importante según el entorno en el cual se aplique como puede ser una empresa financiera.

Hay un sinfín de formas en las que un atacante de la red puede llegar a intervenir con las funciones programadas de un dispositivo IoT o los datos que se trasmiten utilizándolo como medio a dicho dispositivo. Para poder entender algunos de los vectores de ataque se presenta a continuación una imagen en las cuales podemos identificar algunas de las capas que manejan estos dispositivos. (Thales, 2019).

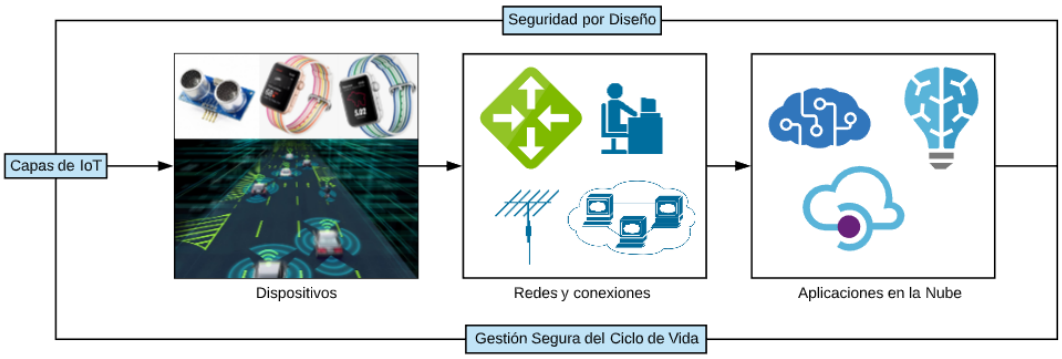

Figura 1. Vectores de ataque de IoT

En vista que existen varios puntos fuera de control de un usuario común es necesario que los proveedores de servicios, los vendedores de dispositivos IoT o incluso las personas que administran la red en el caso de ser una empresa se encarguen de que la información que estos dispositivos manejan posea otro tipo de equipos dedicados a la seguridad o codificación para que no se pueda acceder a dicha información a menos que se tengan las credenciales prudentes para darle un buen uso, brindando un nivel de privacidad a los datos que se transmiten. Es importante definir qué parte se debe proteger como se mencionó con anterioridad por lo cual dos de los principales pilares a tomar en cuenta son los equipos conectados a la red y los datos del IoT que se están transmitiendo, ya sean en reposo los cuales hacen referencia a los que se encuentran dentro de los dispositivos o dentro de la nube o los datos en movimiento los cuales son específicamente los que se presentan en la red.

Un ejemplo de ellos puede ser brindado por Gemalto, el cual es una empresa de seguridad internacional que a principios del año 2019 fue adquirida por Thales, que uniendo los activos digitales que disponían en ese momento lograron convertirse en líder en lo que refiere a los entornos de seguridad digital.

Estos equipos ya sean mediante hardware o software brindaban una posibilidad a fabricantes de equipos originales o incluso a operadores de redes móviles a tener una capa de seguridad adicional en sus equipos.

Algunas de las características que se pueden presentar en estos equipos son:

- **SIM optimizada principalmente para M2M:** El cual da la posibilidad de acceder a un token completamente fuerte para el manejo de los equipos IoT con la ayuda de aplicaciones celulares, a la vez que la información se cifra y verifica los datos de ingreso al equipo dando un nivel extra a redes móviles. (Thales, 2019).

- **Elementos de seguridad por Cinterion:** Este haría referencia a un componente de hardware el cual viene integrado dentro de los dispositivos IoT proporcionando un nivel adicional a la protección en cuanto a la periferia para el manejo de las aplicaciones en el entorno de esta tecnología. (Thales, 2019).

- **Implementación de módulos de seguridad basados en hardware:** Estos módulos conocidos como HSM por sus siglas en ingles son totalmente confiables para la protección de las llaves o tokens que se usan para el manejo de los dispositivos IoT almacenándolas en servidores u otro sistema no vinculado a la red, los cuales son entornos de confianza para lograr proteger la infraestructura. (Thales, 2019).

- **Uso de un administrador de llaves confiable:** Esto se maneja mediante el aprovechamiento de la opción anterior de los HSM para autenticar los dispositivos IoT, logrando así manejar un intercambio seguro dentro de la red evitando los intrusos o equipos no autorizados en la red. (Thales, 2019).

- **Control de entornos IP:** Brindar una seguridad extra para evitar la ingeniería inversa en cuanto a la información que se envía durante la utilización de los equipos. (Thales, 2019).

2.1.2 Privacidad

A pesar de que la mayoría de los usuarios finales son conocedores de los problemas de seguridad que con llevan la tecnología de equipos IoT en cuanto a la privacidad se refiere un 62% del grupo indico que no sería un problema para tomar en cuenta ni se frenaría el uso de estos dispositivos. (Albors, 2018).

Cuando este tipo de tecnología fue implementado poco después los ataques a estos equipos se tornaron cada vez más normales llegando incluso a dejar apartadas las medidas de seguridad que se implementarían para evitar otro ataque a futuro, sino pensar en que sucedería durante el siguiente ataque y cuantos equipos serian intervenidos por el atacante. En vista que esta tecnología no contaba con una garantía solida en cuanto a la seguridad era importante denotar que a futuro existirían aumentos en costos para implementar algún tipo de protección, llegando incluso en una incrementación del 300% en cuanto al costo de aplicar estos cambios.

Los dispositivos que son conectados de tal manera que no posean gran seguridad presentaran vulnerabilidades muy sencillas de aprovechar por parte de terceros o delincuentes informáticos los cuales buscaran realizar Botnets para usarlos con un beneficio propio de ellos.

Estos pueden ser utilizados con ataques tan conocidos como Mirai, utilizados para el minado de las criptomonedas, extorción con la información recopilada, y otro tipo de numerosos y equívocos usos que se les puede dar a estos dispositivos y como se mencionó con anterioridad hay tantos equipos ya implementados sin seguridad aplicada de los cuales los atacantes pueden sacar provecho. Esto llegando a ser tan crítico e inesperado que por ejemplo se conoce del robo de datos de un casino el cual su red fue vulnerada por medio de un termostato inteligente, llegando a obtener información de sus apostadores y subirlos a la nube para que todos puedan acceder a ella. (Albors, 2018).

El problema principal es que se busca optimizar el tiempo del que depende una persona para cierto tipos de actividades llegando a tener prácticamente en cualquier hogar algún tipo de dispositivo inteligente el cual pueda ser vulnerado, desde televisiones Smart, cámaras que se manejan por el protocolo IP,

dispositivos para la grabación de entornos, entre un sinfín de dispositivos que ni si quiera se podría imaginar, dando como resultado millones de puertas abiertas y vulnerabilidades sin parches conocidos a los cuales por una mala gestión al usar estos equipos se debe enfrentar una persona la cual desconoce de todos estos riesgos.

Llegando a dividir estos dispositivos en aquellos que poseen pocas o casi nulas implementaciones de seguridad a equipos completamente configurables para poder protegernos de estas vulnerabilidades. Sin embargo, un usuario podría llegar a la fatídica idea de incluso teniendo la posibilidad de modificar la configuración de un equipo no hacerla debido a que este funciona y cumple con la necesidad para la cual este fue obtenido.

Por otro lado, tenemos los dispositivos que no pueden ser modificados o han sido completamente olvidados por los fabricantes, por lo cual para estos es necesario realizar periódicas revisiones a su funcionamiento, pero no al dispositivo como tal sino al entorno al cual se conecta dentro de la red restringiendo los permisos para evitar conexiones de equipos desconocidos.

2.1.3 Interoperabilidad

En un inicio lo que se buscó al implementar el internet al alcance de toda la sociedad fue con un solo objetivo el cual era implementar una plataforma abierta y que pueda ser usada por una cantidad grande de usuarios, esto principalmente con el fin de que puedan comunicarse sin importar el lugar o el tiempo, realizar compartición de archivos o información libremente sin irrumpir los derechos planteados en un inicio. Para ello se crearon estándares y protocolos para que cualquier persona o grupo de personas se pudiera sumar a esta red con ayuda de sus servidores.

Dentro del mismo lapso se buscó estandarizar el hardware con el cual se lograba la conectividad para las redes, ya sea mediante el uso de cable o de manera inalámbrica, a su vez se creó un lenguaje único para este el cual era HTML para poder mostrar el contenido de las existentes páginas web, con ello que puedan

ser leídas y mostradas en cualquier dispositivo, ya sea móvil o un computador. (Rodríguez, 2020). Gracias a todo lo antes mencionado se logró una interoperabilidad dentro del internet, eliminando las distinciones de las marcas o el fabricante como tal del dispositivo.

Dentro de lo que es el internet tradicional que manejamos todos los días el término de la interoperabilidad es posible definirlo como uno de los valores principales más básicos que se debe tener, dado que este es utilizado como un requisito para el funcionamiento o conectividad que se va a tener dentro de una red, dando a entender que es semejante a un idioma en el cual los dispositivos hablaran dentro de la red, siendo este el principal objetivo marcado para cualquier tipo de fabricante que desee utilizar un equipo dentro del internet, todo esto centrado principalmente en la estandarización brindada por el grupo de trabajo en ingeniería de internet o conocido por sus siglas como IETF.

La interoperabilidad llega a ser uno de los pilares más importantes al momento de implementar un equipo dentro de la red, ya que según la manera en la cual esta está basada afectará directamente a la manera en la que otros usuarios o dispositivos se puedan conectar, compartir, comunicarse e innovar. (Internet Society, 2015).

Este punto es tan importarte que si se llega a crear una plataforma o aplicación de manera más cerrada y que no pueda interactuar correctamente debido a que se centralice para un cierto objetivo o servicio, afectara de manera directa a los beneficios que pueda llegar a traer esta tecnología como pueden ser sociales, económicos o políticos los cuales su accedo es brindado a la totalidad gracias al internet.

Sin embargo, a pesar de todo lo mencionado con anterioridad los fabricantes buscan mejorar o consolidar sus propios dispositivos o plataformas buscando innovar y enfocándolos más en sistemas propietarios más que en la interoperabilidad con otros equipos. (Rodríguez, 2020).

Por otro lado, existe un documento el cual es “Advancing IoT Platforms Interoperability” el cual indica que es necesario enfocarse solo en algunos aspectos de la interoperabilidad no en los siete niveles en los cuales este puede inferir, entre ellos están:

- **Técnica:** Asociada principalmente a los protocolos utilizados para infraestructura y comunicación.
- **Sintáctica:** Asociados con los formatos que se utilizan para los datos y las codificaciones.
- **Organizacional:** Esta asociada a la posibilidad que tiene una empresa para comunicarse de manera efectiva.

2.1.4 Estándares

La aparición de esta tecnología y todos los dispositivos de IoT que han venido con ella plantea una serie de desafíos bastante grandes debido a que surgen nuevas preguntas sobre como ira de la mano el aspecto regulatorio y la parte legal debido al tráfico de información que pueden llegar a tener durante la comunicación de los equipos. Incluso llegando a tener preocupaciones con los derechos civiles que pueden llegar a implicar el uso de los dispositivos IoT.

Esto se debe principalmente a que siempre la tecnología ha avanzado mucho más rápido y de manera más extensa que las políticas que controlan la misma y es muy notable en algunos casos en los que no existe ningún control con respecto a una tecnología, un ejemplo claro con respecto a ello son las transmisiones vía IP los cuales a pesar de representar mejoras en algunos aspectos no se puede tener una correcta tarifa o manejo tal, como puede ser en el caso de la telefonía IP frente a la existente.

Es importante tener en cuenta de que no es posible evitar completamente que los datos que se utilizan o se transmiten mediante los dispositivos de IoT sean enviados a través de algunos limites jurisdiccionales debido principalmente a que se manejan por medio de la internet y este mismo medio atraviesa estos límites en un sinfín de casos. (Internet Society, 2015).

Uno de los desafíos más destacados que trae esta tecnología es la aparición de cada vez más dispositivos conectados de manera completamente automática frente a otros dispositivos y sistemas, a su vez estos dispositivos transmitirán una gran cantidad de datos sin la concepción o conocimiento del usuario. Esto haciendo al usuario completamente responsable de los actos o normas que deban cumplir estos equipos en el caso de que la información que se transmita cumpla con un flujo de datos seguro o si estos están siendo manipulados para otros fines no permitidos sin siquiera tener conocimiento alguno de lo ocurrido. Llegando a crear temas cada vez más complicados en vista al creciente avance tecnológico en comparación a las normas que los rigen.

A pesar de que no podemos decir que con el tiempo se solucionaran estos problemas porque es prácticamente imposible decir que algo es seguro en su totalidad, existen estándares a los que un usuario que este sacando provecho de estos dispositivos se puede apegar para dar un mayor nivel de protección, entre algunos puntos para tener en cuenta pueden ser los siguientes.

- Realizar un cifrado de datos con la ayuda de herramientas informáticas dedicadas a la seguridad.
- Aumentar el nivel de autenticación que requiere un usuario para la manipulación o modificación del entorno de estos equipos.
- La aplicación y uso de codificaciones resistentes.
- Utilizar productos aprobados o aplicaciones estandarizados para evitar puertas abiertas que permitan la fuga de datos.

Uno de los puntos más importantes en el caso de aplicarse en una empresa estos dispositivos es el tema de la utilización de equipos que cada empleado pueda traer para su uso desde su propio hogar o BYOD. Esto debido a que al no estar vinculados directamente a la empresa es más posible que sufran de hackeos incluso antes de llegar a la red de la empresa como un computador tradicional.

Sin embargo, existen dispositivos que son más del estilo independiente los cuales no pueden reaccionar a un ataque, ya que no poseen maneras de defenderse como puede ser un sistema de detección o de prevención de los

intrusos o un simple cortafuegos. Para este caso podría ser una solución crear una red independiente en la cual solo se acepten dispositivos previamente identificados separando este tipo de equipos del resto de la red de la empresa. (Banada, 2015)

El riesgo de estos dispositivos es que principalmente estos se encuentran en ubicaciones al aire libre o incluso en ubicaciones remotas dando la posibilidad de que cualquier tercero pueda acceder a ellas de manera física sin mayor inconveniente y una vez que se logró interceptar el dispositivo es muy complicado realizar un cambio dentro de el para aumentar la seguridad, dando como tales problemas a futuro y que aumentarían de manera considerable dependiendo del uso de ese equipo.

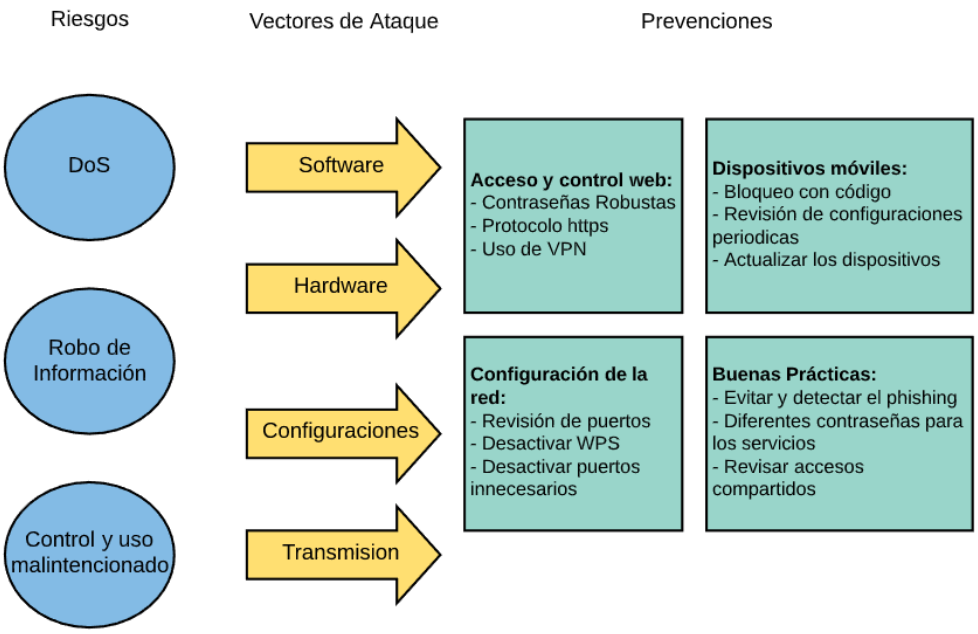

Figura 2. Riesgos y soluciones dispositivos IoT

2.2 Introducción al Blockchain

Al hablar de esta tecnología lo primero de lo que podemos sacar información para entenderla es vincularla a lo que son las criptomonedas ya que como tal las cadenas de bloques aparecieron de manera global en este tema, permitiendo que los usuarios conectados a una red puedan llegar a realizar convenios sin la

necesidad de un intermediario conocido o de confiar con la contraparte con la que se realizaba el trato.

Esta idea surgió a inicio de los años 90, la cual fue planteado principalmente por los científicos Stuart Haber y W. Scott Stonetta los cuales presentaban una innovadora solución computacional y que era practica para aplicarla dentro de documentos digitales basados en un sello de tiempo para evitar una posible modificación o manipulación de terceros. (Binance, 2018).

La idea del sistema el cual proporcionaban buscaba la utilización de una cadena de bloques entrelazados con la seguridad criptográfica para el almacenamiento de dichos documentos con su propio sello de tiempo los cuales un tiempo después se vincularon con el diseño de lo que son los árboles Merkle, permitiendo un nuevo nivel de eficiencia al darle la oportunidad de que varios documentos fueran almacenados y protegidos dentro de un mismo bloque, sin embargo, esta idea no fue muy llamativa para su uso y a pesar de tenerla como patente ésta en el año de 2004 caduco dando rienda suelta a su posible uso el cual fue el bitcoin cuatro años después.

Dentro del año 2004 existió un informático y activista criptográfico con el nombre de Harold Thomas el cual decidido a introducir un nuevo tipo de sistema con las siglas de RPoW, o prueba de trabajo reutilizable. Este tipo de sistema funcionaba básicamente al recibir un token de prueba de trabajo que no se podía intercambiar con algún otro basándose en Hashcash y luego de ello se creaba un token firmado por RSA el cual este si era posible transmitirlo de una persona a otra sin problema alguno.

Este tipo de sistema resolvió un problema fundamental el cual era el doble gasto que se tenía al querer mantener los tokens registrados dentro de una base de un servidor confiable el cual era diseñado para dar la posibilidad al usuario final de verificar la exactitud y la integridad de la información en tiempo real y en cualquier parte del mundo. Este tipo de sistemas fue considerado como uno de los prototipos precursores para iniciar con lo que es la historia de las criptomonedas.

Pasados unos años alrededor del 2008 un grupo de personas lideradas con el nombre de Satoshi Nakamoto hicieron una publicación en una lista de correos criptográficos un libro blanco que dio la posibilidad a un nuevo sistema de control del efectivo electrónico este fue llamado Bitcoin, el cual era descentralizado entre diferentes pares.

Este algoritmo fue basado en la ya mencionada prueba de trabajo por medio de Hashcash, sin embargo, a diferencia de la utilización del confiable RPoW, la protección que se brindó frente a los gastos en Bitcoin fue proporcionada por un innovador protocolo el cual fue descentralizado de igual a igual para poder brindar un seguimiento controlado y una verificación completa de las transacciones que se realizaban durante el intercambio de la comunicación. A manera de resumen se podría decir que los llamados mineros individuales “minaban” bitcoins para poder acceder a una recompensa la cual era basada en el mismo mecanismo ya mencionado de prueba de trabajo para que luego se deba proceder a una verificación con cada uno de los nodos que se encontraban descentralizados por la red.

Dando paso al inicio de esta tecnología la cual fue en el año 2009 en donde el primer bloque de bitcoin fue obtenido y minado por el llamado Satoshi Nakamoto, el cual fue participe de una recompensa de 50 bitcoins y el primer receptor de esta tecnología fue Hal Finney, el cual tuvo la posibilidad de realizar una transacción mediante bitcoins, siendo así la primera del mundo. (Binance, 2018).

2.2.1 Definición Blockchain

También conocida como una cadena de bloques, es uno de los conceptos más llamativos y que suenan alrededor de un sinfín de mercados. Esto se debe a que este tipo de tecnología plantea un punto de vista completamente diferente al que se está acostumbrando, llegando a ser incluso tomado como una tecnología disruptiva, que no únicamente podría afectar a la economía sino extenderse en más ámbitos de nuestro entorno.

Poniendo un ejemplo del porque este tipo de tecnología muestra un cambio dentro de la economía se podría tener como punto de vista una entidad bancaria, dando el caso de que una persona necesita enviarle un pago de un tercero, lo que se pensaría normalmente es que este tipo de transacción para ser realizada correctamente y de manera segura se debe de realizar por medio de una entidad bancaria, en el cual esta entidad deberá ser participe como intermediario para resolver este tipo de transacción a la vez que de muchas otras semejantes a esta, haciendo que todo tipo de movimiento económico sea centralizado de un lado hacia el otro. A este punto la entidad restara el valor a ser transferido de la cuenta bancaria de la persona para enviarlos a la cuenta del tercero y de ser necesario confirmar a otro banco la transacción que se ha realizado.

Este tipo de transacción no se ha necesitado como tal un intercambio de dinero o efectivo de manera física de un lado a otro sino que se ha realizado un cambio de balance dentro de las cuentas de los usuarios participes de esta transferencia, por un lado se puede decir que es un problema resuelto de manera óptima sin ninguna interferencia entre el medio, sin embargo si nos damos cuenta ninguno de los usuarios que realizo esta transacción tuvo algún control o voto durante el proceso que se realizó, en vista que la entidad bancaria tuvo durante todo este proceso la información necesaria. Si nos damos cuenta de ello los bancos tienen completo control del cómo realizar y cuando este tipo de transacción, y los usuarios participes deben estar completamente de acuerdo con las condiciones que estos planteen como pueden ser las comisiones por realizar este proceso.

Esta es la parte esencial en la cual pone de parte esta nueva tecnología buscando eliminar a los intermediarios y así evitando toda centralización que se tiene en este tipo de gestión. En este ejemplo todo el control pasaría a los usuarios que desean realizar esta transacción convirtiendo a los usuarios finales en una entidad bancaria con más de miles de millones de nodos los cuales pueden ser partícipes y gestores de las cuentas de banco.

De manera general podríamos llamar a la cadena de bloques como un libro de cuentas en la cual se almacenan estos registros a manera de bloques los cuales se encontrarán entrelazados y completamente cifrados para evitar así

modificaciones o robos de la información durante la transacción dando un nivel superior a las transacciones.

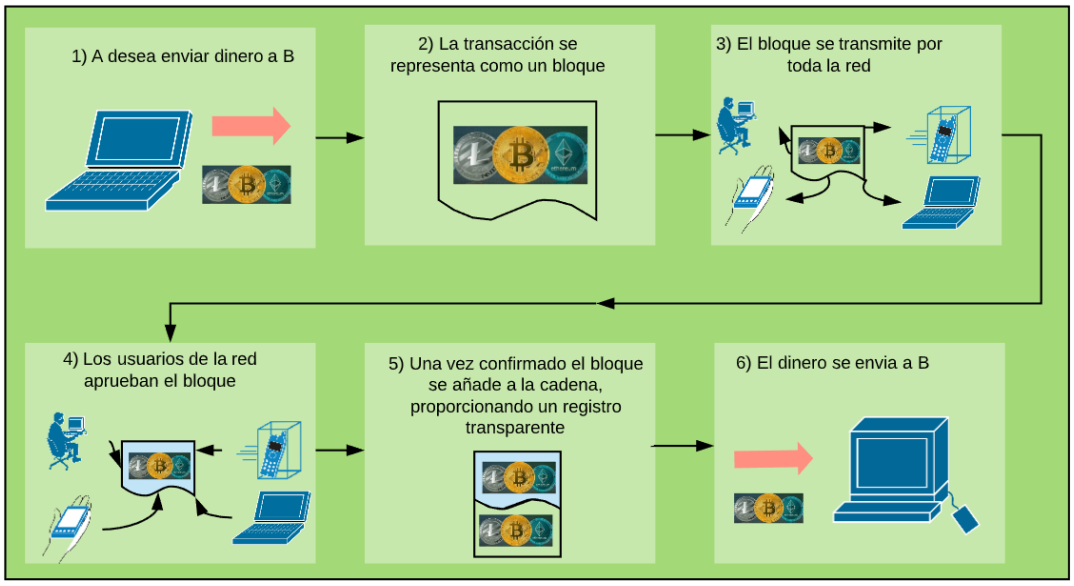

Figura 3. Funcionamiento del Blockchain

Por lo cual podemos decir que uno de los ideales para la creación de este tipo de tecnología fue crear un sistema descentralizado en el cual cada uno de los usuarios pueda ser participe del cambio global que se avecina y no únicamente ser espectadores que no tenían voto en algunos casos, a este podríamos llamar como uno de los elementos que tiene cualquier tipo de Blockchain público. (Champagne, 2014).

Hay que mencionar que las personas que desarrollan este tipo de tecnologías o modelos para negocios basados en Blockchain públicos son por lo general usuarios que luego de vivir en un sistema centralizado, este ha fallado en varios aspectos ya sea a nivel social como también a un nivel global. Los principales aportadores de estas tecnologías son personas que buscan encontrar una manera distinta de realizar el cambio, pensando en la tecnología como una fiel colaboradora y como objetivo del mismo criterio plantear una tecnología disruptiva el cual afecte y mejore a todos los modelos de negocios actuales.

Por todas las razones mencionadas con anterioridad de Blockchain es posible decir que no únicamente es una tecnología, sino que busca ser una razón o incluso manejarse como un instrumento para el cambio social.

La tecnología de Blockchain se apoya principalmente con la ayuda de su comunidad, las matemáticas las cuales utiliza en la criptografía aplicada para poseer una base de datos de manera segura, determinando cuando es válido o real con respecto a los valores que se transmiten sin la necesidad de contactar a una entidad central para coordinarlo como se tienen en las bases de datos tradicionales.

Por lo cual podemos entrelazar todo lo que es el Blockchain con lo que es el internet en vista a los beneficios que busca traer consigo, separando al internet incluso ya en dos partes distintas las cuales podemos llamar como el internet de la información y por otra parte el internet del valor. En el cual en el primer caso este estaría más dirigido a los estándares que son abiertos a los usuarios permitiendo la transmisión y comunicación de los datos alrededor de todo el mundo dando la posibilidad a modelos de negocios tan famosos como puede ser Amazon.

Por otro lado, tenemos el internet de valor creado sobre los mismos estándares abiertos, pero este mayormente enforcado a la tecnología Blockchain, este dando la posibilidad de transmitir información, pero sin la necesidad del ente intermedio, como puede ser el caso de PayPal, sino que se busca realizar una transacción P2P comprobando la transacción y que esta sea única evitando que se repita el gasto del mismo valor varias veces, como si se realizara un registro pero este sería basado en un software el cual es descargado por todos los usuarios que deseen manejar este tipo de sistema, haciendo participes a todos los involucrados en la transacción y dándoles la posibilidad para la revisión de todo el proceso.

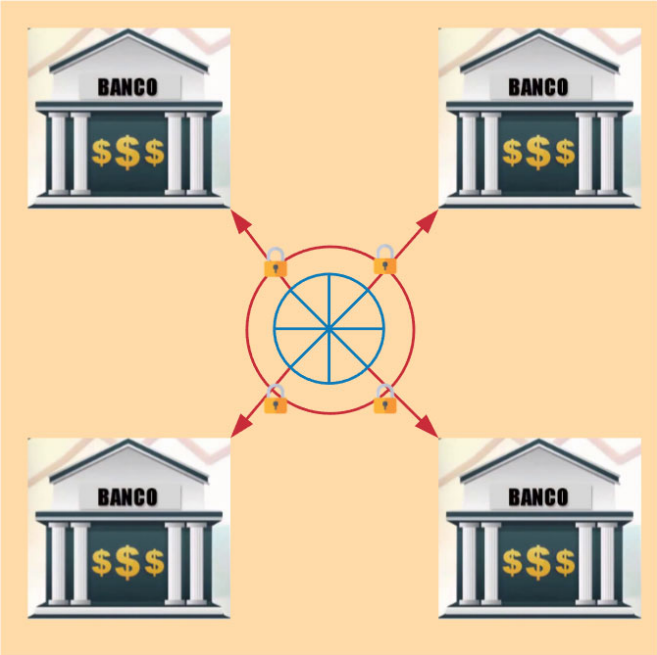

Figura 4. Centralización caso financiero

Pero para entender todo lo que es la tecnología debemos basarnos en el corazón de esta, la cual es la criptografía, ya que toda información o data que se comparte mediante Blockchain por cualquier red de ordenadores es transmitida de forma encriptada sin ningún tipo de jerarquía en base a los equipos, poniéndolo como un código o clave secreta que puede dar a conocer únicamente al dispositivo o usuario al que se le está enviando dicha información.

La criptografía surgió durante la Segunda Guerra mundial en la cual los gobiernos fueron capaces de identificar la gran relevancia que tenía el codificar y descodificar la información que se enviaban. En esa época un matemático británico con el nombre de Alan Turing fue quien descifro los códigos de “Enigma“, la cual era la principal máquina que se utilizaba por parte de los alemanes para informar sus mensajes, considerándolo como el padre de la criptografía. (BBVA, 2017).

En cuanto a lo que son los algoritmos para encriptación fue en 1976 cuando Whitfield Diffie y Martin Hellman crearon como tal el algoritmo llamado Diffie-Hellman, el cual proponía como procedimiento el dividir las claves que se tenían en dos, de modo que se tenga una clave privada y otra publica para poder utilizarla. Para este proceso la clave publica se utilizaría principalmente para encriptar la información, sin embargo, para poder desencriptarla se necesitaría de la clave privada. Otro de los pilares para los algoritmos fue la creación de los árboles de Merkle el cual surgió en un tiempo similar al método antes mencionado, posicionándolos como los creadores de la criptografía basada en una clave pública. (BBVA, 2017).

Con estas técnicas ya consolidadas y usándolas como base fueron las que empujaron a la creación del Blockchain y el bitcoin basándose como ya se mencionó en un manifiesto cripto-anarquista, estos tipos de fenómenos fueron marcados como un movimiento 'ciberpunk' el cual buscaba como objetivo el defender la libertad de expresión, el poder acceder a la información con toda privacidad como pilares y estos serían transmitidos a lo largo del futuro con la ayuda de la tecnología y la criptografía.

2.2.2 Ethereum

Alrededor del año 2013 un programador y cofundador de la revista Bitcoin llamado Vitalik Buterin, menciono que el Bitcoin modo tal necesitaba un tipo de lenguaje de scripting para poder realizar la creación de aplicaciones no centralizadas. Sin embargo, esta idea no fue muy aceptada por el resto de la comunidad y por su propia cuenta inició con un estudio y desarrollo de una plataforma de computación la cual era distribuida y se basaba completamente en el Blockchain la cual fue llamada como Ethereum, esta presentaba la funcionalidad de scripting que él deseaba con anterioridad y fue llamada como contratos inteligentes.

Este tipo de tecnología llamados contratos inteligentes son programas computacionales o scripts que eran capaces de implementa y ejecutar una cadena de bloques Ethereum, los cuales eran utilizados para realizar transacciones siempre y cuando se cumplan condiciones que se planteaban en un inicio. Este tipo de tecnología manejaba lenguajes en específico y se compilaban por medio de un código de bytes, estos eran leídos y ejecutados por una máquina virtual completa de Turing descentralizada.

Características

Luego de comprender todo lo que conlleva el termino Blockchain se puede entrar más a fondo detallando como características las siguientes:

- Es considerado sistema seguro, ya que se basa en el uso de la criptografía para la comunicación de datos.
- Las transacciones o comunicaciones se centran en los conocidos como bloques, en los cuales los datos se almacenan de manera cronológica.
- Una vez aceptado el conceso de envío la información no puede ser modificada ni borrada, sin embargo, si puede ser consultada en cualquier instante de tiempo.
- El uso de Blockchain puede ser privado o público según se necesite, permitiendo incluso la consulta de datos en específico con la ayuda de una clave generada.

2.3 Elementos que definen una Blockchain

Principalmente podemos definir como elementos del Blockchain a los siguientes:

1. **Criptografía de clave pública**: A esta la podemos definir como la criptografía asimétrica, la cual se basa en la implementación o uso de una curva elíptica principalmente para la mejora del rendimiento frente a implementaciones que se utilizaban en la anterioridad como puede ser RSA. Realizando de esta manera la validación y autenticación del emisor de la información. (Rojo, 2020)

Para las implementaciones que más han destacado en el entorno actual como es Bitcoin y Ethereum, este tipo de comprobación se realiza mediante la comparación de las llaves públicas de los remitentes confrontándolo con el elemento firmado con la clave privada.

2. **Base de datos distribuida:** Cada uno de los nodos participantes en la red está encargado de replicar en su totalidad la base de datos al querer pertenecer a la red de Blockchain como tal. Mediante este proceso de réplica es en el cual un nodo pasa a ser parte de la red cuando este se sincroniza. Únicamente cuando el nodo esta sincronizado podrá ser parte de las operaciones que se realizan en el Blockchain. Uno de los puntos a denotar es que la base de datos distribuida es alimentada por todos estos bloques, es decir que, si la transacción que se está realizando no es confirmada incluyéndola en un bloque valido o sincronizado, esta será rechazada considerándola como una conexión no valida dentro del Blockchain. (Rojo, 2020)

3. **Algoritmos de consenso:** Podríamos definirlo como el elemento más importante, ya que este es el diferencial principal frente al resto de los sistemas distribuidos y como tal Blockchain es el algoritmo de consenso que se utiliza. Este principalmente creando algún tipo de recompensa para invitar a los usuarios a ser partícipes de las transacciones también conocidos como los mineros los cuales son los principales encargados de la creación de los bloques que se utilizan en la cadena. (Rojo, 2020)

Algunos de los modelos más utilizados por el momento son los siguientes:

- **Prueba de trabajo (PoW)**

Este siendo el algoritmo más destacado debido a su uso dentro de Bitcoin y la versión que se utiliza de manera estable de Ethereum. Este tipo de modelo está orientado a lo que son las redes públicas.

Este tipo de algoritmo se basa en la utilización de un hash y basándose en este se vincularán con su bloque siguiente para formar la cadena con un valor único.

- **Prueba de Autoridad (PoA):**

Este tipo de algoritmo es principalmente utilizado por Ehtereum cuando se busca gestionar redes privadas. Este tipo de algoritmo busca el acelerar la subida de los bloques a la cadena y a su vez las transacciones, esto principalmente debido a que se definen las llamadas autoridades y estas se centraran en la parte a la cual fueron asignados dichos nodos.

Cada una de las autoridades definidas en el proceso de transacción posee una clave privada única que le permite realizar las firmas o validaciones dentro de la red para poder así realizar una transacción segura. Por otra parte, lo definido como público se distribuirá de igual manera por toda la red al resto de las autoridades.

A continuación, se podrá tener un detalle más técnico de cada uno de los modelos existentes a la vez que ver un punto más objetivo para poder denotar cuál de estos pueden funcionar de manera óptima para proteger los datos enviados por medio de los dispositivos de IoT.

3. Desarrollo

Dentro de este apartado podremos entender mejor el funcionamiento de los modelos que existen para el uso del Blockchain a su vez que separarlos según sea la necesidad que se tenga para los equipos IoT.

Existen vario modelos para poder aplicar lo que es la tecnología de Blockchain y se pueden diferenciar según la aplicación que se le va a dar, como puede ser el tipo de transacción, la cantidad de transacciones que se van a realizar con esta tecnología, la escalabilidad que va a tener la red en la que es aplicada, la tolerancia que se va a necesitar, entre otros.

3.1 Prueba de Trabajo (PoW)

Este tipo de algoritmo de consenso es principalmente utilizado en lo que son las redes de Blockchain. Este algoritmo se utiliza principalmente para la confirmación de las transacciones y con ello formar nuevos bloques verificados para poder agregarlos a la cadena.

Para este caso son utilizados como tal a los usuarios que pueden ser conocidos como los mineros dentro de la red de Blockchain estos principalmente resolviendo las transacciones que se disponen en la red para poder obtener una recompensa que pueden ser por ejemplo los bitcoins.

Dentro de la red los usuarios que son partícipes realizan un intercambio de los llamados tokens digitales. Un dato importante es que todos los bloques que se van formando los reúne una base de datos descentralizada, sin embargo, para este modelo es necesario tener en cuenta que cada uno de los bloques debe ser confirmado y organizado para dar un buen nivel de seguridad al momento de añadirlos a la cadena. (Tar, 2019). Como ya se ha mencionado este tipo de proceso se basa en la transmisión por nodos siendo estos los llamados mineros dándole el nombre como tal a la formación como minería.

Los principios de este proceso es el realizar trabajos fundamentales con respecto a problemas matemáticos buscando que el minero entregue una solución fácil de comprobar para solventar cierto problema. Pero al mencionar lo que son los problemas matemáticos nos surge la pregunta de que son o como se enviara la respuesta.

Por lo general estos tipos de acertijos matemático que se envían a los mineros requieren una gran cantidad de poder de cálculo para que estos puedan ser resueltos, ya que si no fuera el caso cualquiera podría acceder a una gran cantidad de recompensas sin trabajo aparente.

Para este tipo de modelo existen varios acertijos posibles como pueden ser:

- **Función Hash**

Este término hash es definido como una función criptográfica, en esencia es un algoritmo matemático que es capaz de transformar cualquier tipo de bloque de

datos en una serie de caracteres completamente distinto y que poseen una longitud fija. Este tipo de conversión se realiza independientemente de la cantidad o longitud que se ingresen en un inicio como entrada el valor de tipo hash al momento de salir siempre poseerá una longitud fija. (Donohue, 2014).

Existen varios generadores de códigos hash y entre ellos se podría destacar el hash SHA-1, el cual es una de las funciones que se utilizan en gran cantidad al momento de relacionarlas con la informática, otros pueden ser MD5 y SHA-2, sin embargo hay que tener en cuenta que debido a su gran utilización existen ya presentes algunos tipos de decodificadores los cuales harían totalmente inútiles este tipos de codificaciones, como puede ser el caso de MD5 siendo ya algoritmos prácticamente inutilizados a menos que se busque dar otro tipo de soluciones para solventar este tipo de problemas en redes que ya los tengan implementados.

Ejemplo MD5:

Mensaje original: Hola, este es un ejemplo

Codificación MD5: b798fb0a87f009b8040c2030314c9ff7

Ejemplo SHA-1:

Mensaje original: Hola, este es un ejemplo

Codificación SHA-1: fdf7ecdd7f381a2a93dc8d78260105a085475e80

Mensaje original: hola

Codificación SHA-1: 99800b85d3383e3a2fb45eb7d0066a4879a9dad0

Como se puede ver a pesar de ser el mismo mensaje el resultado es diferente esto principalmente a que el algoritmo de codificación posee procesos distintos y se diferenciaran a su vez las palabras o letras que se tengan con mayúsculas. Como ya se mencionó con anterioridad es importante denotar que no importa el valor de caracteres que se ingresen en un inicio siempre tendrán una longitud

fija al momento de transformar el mensaje, para el caso de SHA-1 serían de 40 al momento de transformarse.

Estos tipos de encriptaciones son usados para un sinfín de aplicaciones principalmente para el uso de contraseñas como pueden ser en sitios web, esto debido a que un sitio web no puede permitir que al mostrar las contraseñas sean presentadas en texto plano, porque de ser el caso un programador experimentado que busque robar información tendría un acceso muy sencillo a todas las cuentas.

Para lo cual podemos definir algunos de los requisitos que se requieren para que una función hash pueda ser válida.

1. Podemos definir a la función hash como H(m)
2. Siendo H una función conocida.
3. H(m) siempre deberá enviar una salida de la misma longitud independiente del valor de entrada m.
4. En el caso de que m sea al menos un bit distinto el resultado debe ser totalmente diferente.

Existen hash mucho más complicados como puede ser Script el cual busca ya la combinación de símbolos con los caracteres alfanuméricos que poseen normalmente, esto principalmente para aumentar el nivel de complejidad a usuarios malintencionados que desean desencriptar un mensaje transmitido.

Dando como resultado al modelo de prueba de trabajo, el cual busca enviar mensajes codificados por hash a sus mineros para que estos busquen la manera más optima de descifrarlos por medio de cálculos matemáticos.

- **Factorización de enteros**

Este es un método más sencillo el cual es conocido por casi la mayoría de las personas, este tipo de problemas matemáticos son principalmente utilizados para proteger sistemas de cifrado de clave pública. Para este punto lo único que se busca que los mineros buscan alguna otra manera de presentar un numero como una multiplicación de dos distintos valores para resolver el problema.

- **Protocolo de rompecabezas guiado**

Para este caso se basa en un protocolo en el cual si algún servidor sospecha que se está realizando algún tipo de ataque de denegación de servicio se busca utilizar acertijos criptográficos para poder mitigarlos esto basándose principalmente en disminuir la tasa entrante de las solicitudes para un servicio.

Sin embargo, a pesar de ser una solución llamativa no es completamente eficiente principalmente a que estos tipos de modelos no poseen caminos precisos para determinar el proceso o rompecabezas a seguir para dar con el atacante, tampoco posee un contador eficiente para poder visualizar si el ataque que se está realizando o alguno de los acertijos ya fueron resueltos en otros rompecabezas.

Por lo tanto, el objetivo para este proceso es que los mineros busquen cual es el orden en el identificar el problema que está sucediendo o como tal encontrar una cadena de bloques basándose en el hash que se les estará enviando.

Es importante tener en cuenta que a pesar de que, en algunos casos, aunque el proceso que se le está enviando al minero suene sencillo esto únicamente será en un inicio, debido a que la complejidad de los algoritmos que se necesitaran para poder resolver estos acertijos será cada vez más extensa, esto principalmente para equilibrar el proceso de recompensas por el trabajo que realiza un minero. De tal manera que el proceso quedaría similar al siguiente.

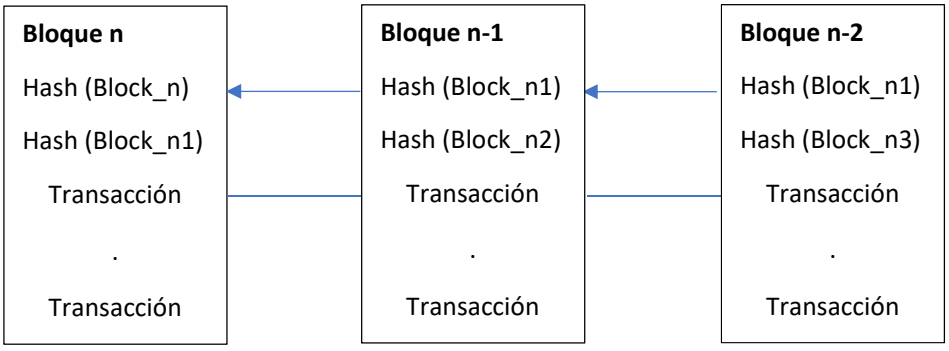

Figura 5. Unión de una cadena de Blockchain

Una vez varios mineros envían sus respuestas se realizarán las verificaciones correspondientes para comprobar primeramente si la solución enviada es la correcta y luego confirmar el bloque con la solución óptima para la cadena de bloques.

El principal problema que se tiene con respecto a este modelo es que los usuarios o mineros requieren de grandes capacidades de hardware incluso llegando a crear dispositivos específicos para este tipo de trabajo para poder continuar recibiendo las recompensas que se tienen por ofrecer, el gasto principal que se tendría seria en la energía que estos equipos consumen aumentando como tal el costo. (Tar, 2019).

Otro problema que se puede tener dentro de este modelo es el ataque del 51%. Este tipo de ataque es conocido como el ataque mayoritario en el cual ya sea un usuario único o un grupo de ellos buscan tener una cantidad mayor para el procesamiento de la minería, llegando a controlar la mayor cantidad de los eventos que se realizan durante la cadena de bloques llegando a monopolizar la generación de los nuevos bloques obteniendo todas las recompensas disponibles limitando los mineros que pueden participar en la red, por otro lado podrían llegar a controlar las transacciones evitando como tal que este se realice al controlar el cómo se unirán los bloques y extendiendo el tiempo en el cual esta información se pueda transmitir. (Tar, 2019).

Sin embargo, este tipo de ataque no es tan rentable porque como se menciono es necesario superar la potencia de todo el resto de los mineros que existe dentro de la red y al realizar esto comprometerían la seguridad de la red como tal llegando a que los usuarios que eran participes de esta la abandonen haciendo que el precio de la criptomoneda que se esté dando en ese momento se desplome haciendo que pierda valor trabajar por las recompensas.

3.2 Prueba de Participación (PoS)

Este tipo de algoritmo también considerado como de consenso aparece principalmente como una alternativa que se tiene para la prueba de trabajo

(PoW) y su principal objetivo es lograr que se tenga un consenso totalmente distribuido. Su primera aparición fue con Peercoin, la cual fue una criptomoneda lanzada el año 2011 por el mes de agosto. (Jiménez, 2019).

Hay que denotar que a pesar de buscar remplazar como tal el anterior algoritmo de prueba de trabajo este tipo se modelo difiere mucho en el funcionamiento a este debido a que en lugar de buscar que los mineros a los que se les enviaba el hash comprueben todas las posibles transacciones sean legitimas la prueba de estaca o de participación busca que un usuario realice algo similar a lo que es una apuesta, mantenga o bloquee lo que son las monedas y a su vez sea el que compruebe la validez de la propiedad que tienen estas. De manera más sencilla podríamos decir que en vez de buscar que los mineros apliquen grandes cantidades de cálculos para resolver un problema matemático, lo que se busca es que se validen los bloques que van a incluir dentro de la red de acuerdo con la participación que tenga cada uno de los involucrados en la red.

Pero nos podemos poner a pensar que existen problemas similares a los que su modelo predecesor tenia, sin embargo, este tipo de algoritmo posee maneras de seleccionar nuevos participantes para la creación de los bloques y logrando así quitar el problema de la centralización que se tendría en el anterior caso donde un solo usuario pueda bloquear una cantidad de las monedas para aumentar su beneficio, este modelo asegura principalmente la cadena de bloques al aumentar un proceso de selección pseudoaleatorio tomando en cuenta varios puntos como puede ser la riqueza que ya ha tenido un nodo durante su participación en la red y a su vez comprobando la antigüedad que tienen las monedas retenidas o ‘apostadas’ para pasarlas por medio de un factor aleatorio. (Jiménez, 2019).

Es importante tomar en consideración que dentro de los modelos de Prueba de Estaca al ser un manejo distinto de los bloques estos en lugar de ser llamados ‘minados’ como era en el caso de su antecesor, sino que los bloques verificados son llamados como ‘forjados’. Por otro lado, es importante denotar que en el caso de las criptomonedas que se utilizan como beneficios o dentro de las transacciones de este tipo de modelo en un inicio son monedas que son

previamente minadas o traídas por medio del modelo de Prueba de Trabajo que luego con el tiempo son cambiadas a este tipo de algoritmo.

El proceso como tal para que los usuarios puedan participar dentro de lo que llamaríamos como proceso de forjación es que en un inicio los usuarios dentro de la red apuesten o bloqueen una cantidad especifica de monedas centrándola como su estaca siendo el caso que mientras más monedas se bloqueen más posibilidades existirán para ser escogidos. Como ya se mencionó el tamaño de la estaca es el principal determinante para que un nodo sea escogido para que realice el proceso de validación logrando así forjar el siguiente bloque de la cadena. Pero al escuchar la principal característica para seleccionar un nodo nos volvemos a plantear el método de centralización, pero como ya se mencionó dentro del proceso normal para escoger los nodos a pesar de existir los nodos con una estaca más grande dentro de la red en comparación a los demás son agregados nodos de manera aleatoria a su vez.

Los dos principales métodos utilizados para evitar la centralización son llamados como “Selección aleatoria de bloques” y “Selección de la edad de la moneda”. (Academy, 2018).

En cuanto al método que se utiliza para seleccionar los bloques aleatorios las principales maneras en las que se realiza la elección de los nodos validadores se comprueban con la combinación de dos puntos siendo el primero el cual posea un valor hash relativamente bajo y el segundo el que tenga la estaca más alta, y como el tamaño de las apuestas o estacas son públicas para todos los participantes de la red es posible llegar a predecir cual de todos los nodos existentes puede ser el siguiente forjador. (Academy, 2018).

El otro método del cual se habló es por medio de seleccionar el nodo según la edad que posea la moneda se basa principalmente en el tiempo que se ha acumulado los tokens que tiene cierto usuario.

En cuanto a la antigüedad como tal de la moneda se realiza por medio de un cálculo matemático sencillo en la cual se debe multiplicar la cantidad de los días que han transcurrido durante el periodo en el que las monedas han sido

acumuladas por el total de las monedas acumuladas. Hay que recalcar que una vez el nodo sea seleccionado y este a su vez realizo el forjado de un nuevo bloque dentro de la cadena de la red la antigüedad que poseía en esa entonces la moneda se deberá restablecer a cero y se da también la penalización de que este nodo debe esperar un periodo de tiempo puntual para poder forjar un nuevo bloque de la cadena, evitando así la centralización de un solo nodo al reducir la probabilidad de que sea escogido entre el resto. (Academy, 2018).

A pesar de que un bloque sea escogido por tener una estaca más grande el valor que se envíe a la red como el nuevo bloque a validar en el caso de que la solución sea errónea si la solución como tal no es la correcta no se tomara en cuenta a pesar de haber sido el nodo escogido validando así la transacción que se realiza, si el caso es el contrario y la respuesta es la correcta se procederá a firmar el bloque y validarlo como correcto lo cual hará que este nuevo bloque sea agregado a la cadena.

Una vez se agregue dicho bloque el nodo que fue participe de dar la respuesta será recompensado con la comisión de la transacción la cual fue asignada para esa parte del bloque en el que ocurría la transacción.

En el caso de que un nodo que este siendo participe de la red ya no desea ser forjador, el lugar que este estaba ocupando a la vez que las recompensas que tenía asignadas serán liberadas luego de un periodo de tiempo, lo que le da la oportunidad a la red que durante este tiempo se realice una verificación de cada uno de los bloque comprobando la validez de cada uno de ellos que se hayan agregado a la cadena por ese nodo. (Academy, 2018).

Otro punto para tomar en cuenta es que en el caso de las criptomonedas se utilizan diferentes variaciones del algoritmo de Prueba de Estaca y el conjunto tanto de métodos como de reglas que se utilizan en combinación y a su vez estos son escogidos según el mercado en el que se apliquen siendo que se deberá pensar primero en la mejor combinación para la moneda como tal y los usuarios que se van a tener en la red.

Para este tipo de modelo existen diferentes variaciones que son principalmente cambios para poder aplicar para otro tipo de criptomonedas como pueden ser algunas de las más importantes Binance Coin, Cosmos, Neo, entre algunas otras, representando ya un 3,52% de lo que es el mercado en general. (Jiménez, 2019). Algunas de las variaciones que existen para este modelo pueden ser:

- Prueba de Participación Anónima (PoSA)
- Prueba de Velocidad de Estaca (PoSV)
- Prueba de Importancia (PoI)

Para el caso de seguridad en este tipo de modelos la estaca como tal puede funcionar como un tipo de motivador financiero para que el usuario dueño de la estaca o el nodo como tal que está forjando no realice validaciones ni creaciones fraudulentas de las transacciones que se están dando en la red.

En el caso de que la red detecte algún tipo de transacción fraudulenta validada por un nodo, este nodo forjador será penalizado perdiendo una parte que posee por haber participado dentro de la red y a su vez se le negara el derecho de volver a ser participe como nodo forjador en el futuro de la misma red.

Por lo cual, en el caso de que se haya creado una estaca muy grande para realizar una transacción fraudulenta la perdida de la recompensa seria mucho mayor, llegando incluso a que la perdida que tenga por su participación sea mayor a las monedas que aposto en un inicio.

Por otro parte como ya se mencionó con anterioridad para que un nodo como tal posea el control total de una red y pueda aprobar transacciones fraudulentas sin problema dicho nodo deberá tener la mayor participación dentro de la cadena de bloques que se está forjando en la red, conocido como el ataque del 51%. Pero como ya se mencionó dicho control no siempre tendrá el mismo valor debido a que dependerá meramente del valor que tenga la criptomoneda y para que pueda llegar a tener esta participación obtener el valor de la oferta circulante de la red el costo sería mucho mayor al beneficio que pueda obtener por las transacciones erróneas. (Binance Academy, 2018).

En comparación a su predecesor el algoritmo de Prueba de Trabajo este modelo basado en la participación de un usuario tiene dos ventajas a denotar el cual son la eficiencia energética al no contar con grandes cantidades de trabajo al momento de querer resolver problemas matemáticos y la seguridad que se tiene al obtener nodos pseudoaleatorios de todos los disponibles que se encuentren en la red de la cadena de bloques.

Este modelo es mucho más rentable y recomendado a los usuarios que deseen ser partícipes como nodos ya que es un algoritmo más fácil y asequible para ser aplicado. Esto más el proceso de selección de manera aleatoria da como resultado una red mucho más descentralizada en comparación, ya que no es necesario tener grandes equipos costosos para resolver problemas matemáticos a los cuales pocos nodos tienen acceso.

Además de que dentro de este modelo no es tan necesario realizar lanzamientos de nuevos tipos de monedas para poder brindar más recompensas haciendo que el precio de una moneda no varíe tanto, sino que se mantenga estable durante la transacción.

3.3 Prueba de Autoridad (PoA)

Este tipo de algoritmos fue dirigido principalmente para la creación y diseños de Blockchain privadas esto debido a que este tipo de solución era practica y eficiente al momento de implementarla. Este tipo de modelo surgió como un ideal de Gavin Wood quien fue cofundador de lo que es Ethereum. Este tipo de algoritmo de consenso es totalmente distinto a cómo funcionan sus predecesores los cuales son Prueba de Trabajo y Prueba de Estaca. La principal diferencia que posee este algoritmo es que busca el aprovechar las identidades reales de los participantes de la red permitiendo una validación segura dentro de la cadena de bloques. (Bit2me Academy, 2020).

Esto representa una seguridad enorme ya que los participantes o validadores ponen en juego su identidad real y a su vez la reputación que han ganado como la garantía de que su validación del bloque es transparente. El cual representa

como tal a un proceso de selección totalmente arbitrario de los validadores que son seleccionados como confiables. Este tipo de situación es claramente distinto a como podría ser la minería en el caso de la Prueba de Trabajo, pero muestran semejanza a como serían los esquemas con los que trabaja el algoritmo de Prueba de Estaca. (Bit2me Academy, 2020).

Es importante tener en cuenta que para este tipo de modelo los validadores llegan a ser un número limitado de personas mostrando como tal una clara ventaja como tal para el Blockchain al querer hablar de escalabilidad. Este tipo de características llegaría dar una gran ventaja para aplicaciones en las cuales la velocidad que se requiere para la transacción es primordial. Además de segmentar totalmente los permisos que se dan a los usuarios que están encargados de los nodos de validación al ser que esto son previamente seleccionados según la confianza que tengan con el tiempo.

Es importante tener en cuenta que en la actualidad el algoritmo más utilizado es la Prueba de Trabajo el cual es frecuentemente mencionado dentro de los Bitcoin al ser uno de los más confiables y seguros que pueden presentarse en el mercado en la actualidad. Sin embargo, el problema que presenta este tipo de modelo es su escalabilidad. Este problema es debido a que en sus aplicaciones en las Blockchain muestran un rendimiento limitado al momento de tratar con las transacciones por segundo que pueden manejar. Este problema surge por la misma manera en la cual esta predispuesto este modelo el cual se basa en una red de nodos distribuidos, estos a su vez necesitan estar completamente de acuerdo o llegar a un consenso con la actual Blockchain que estén trabajando y finalmente comprobar y verificar los estados que posee cada uno de los nodos distribuidos.

Por lo cual, este algoritmo requiere que antes de agregar un nuevo bloque dentro de la cadena el resto de los bloques agregados por los nodos sean verificados y aprobados por casi la totalidad de los mineros, dando como resultado un sistema económico totalmente seguro y descentralizado hasta cierto punto, pero por otra parte muestra una desventaja en su potencial para ser aplicados a grandes escalas. (Binance Academy, 2020).

Como ya se mencionó para este modelo al poder seleccionar los validadores que se tendrán controlando los bloques dentro de la cadena de la red este algoritmo podrá ser aplicado para una variedad extremadamente grande de escenarios e incluso poder considerar opciones de alto valor dentro de aplicaciones logísticas debido a la confiabilidad que se tendría en la red privada, como puede ser el caso de una cadena de suministros.

Este tipo de algoritmo de consenso está dirigido principalmente para las empresas debido a que apunta a que se tenga una completa privacidad al seleccionar a los participantes o moderadores de los nodos mientras que se pueden empapar de los beneficios que trae consigo la tecnología de Blockchain.

Uno de los ejemplos más grandes y conocidos que se puede tener del modelo de Prueba de Autoridad es la plataforma conocida como Azure la cual puede proporcionar diversas soluciones para las redes privadas de las empresas, a la vez que este tipo de sistema no necesita de una moneda como tal previamente creada al no tener nada que ver con lo que es la minería. (Binance Academy, 2020).

Existen varios lineamientos que se deben tomar en cuenta al momento de querer utilizar este tipo de algoritmo, los cuales son:

- Es necesario validar y confirmar las identidades reales de los que participaran como los nodos de la red.
- El candidato que va a ser seleccionado como validador dentro de la red deberá estar completamente de acuerdo que para este modelo necesitará invertir dinero y tener en claro que su reputación estará en juego.
- Crear un proceso complejo para poder reducir los riesgos que se puedan tener al momento de seleccionar los validadores y lograr así incentivar un trato con la persona a largo plazo.
- A pesar de que se buscan personas confiables y conocidas todos los participantes que se deseen incluir en la red deben ser evaluador de una manera estandarizada para que todos tengan las mismas posibilidades.

El proceso que se manejará para marcar la reputación de cada uno de los participantes y dueños de los nodos debe tener una certeza total, a su vez que los estándares que los califiquen deben ser complejos para que no cualquiera pueda llegar a obtenerlos ni abandonarlos con facilidad. Esto principalmente para eliminar a terceros que busquen aprovecharse de la oportunidad. De esta manera se garantizará la integridad y confiabilidad de los participantes y con ello de la red de Blockchain como tal.

Una de las principales desventajas que muestra el modelo de Prueba de Autoridad es que se deberá renunciar totalmente al termino que conlleva la descentralización de la cadena. Por lo cual, este modelo no fue más que otro que buscar hacer que los sistemas que ya son centralizados tengan una eficiencia mucho mayor frente a la que ya se tenía con anterioridad. En el caso de querer agregar a nuevos nodos se debe tener en cuenta que gran peso del voto recae sobre los participantes previos de la cadena.

En el caso de que se tenga algún problema dentro de la fiabilidad de un bloque o la transparencia que se esté teniendo dentro de la red se deberá revisar en que nodo fue validado y al tener una identidad publica en cada uno de ellos en el caso de que existir algún inconveniente el problema recaerá directamente a la persona o institución encargada del nodo afectando totalmente la reputación que esta tenga llegando incluso a destruirla por completo y haciendo que en futuros proyectos de Blockchain ya no sea tomada en cuenta. Sin embargo, esta también puede ser tomada como ventaja, ya que al tener toda la presión sobre sus hombros cada nodo deberá velar por el correcto funcionamiento, la transparencia que se tendrá y a su vez la confiabilidad de la transacción durante su operación.

A pesar de que suene totalmente seguro al ser moderadores conocidos públicamente esto puede llegar a ser un riesgo por el mismo caso, esto es debido a que siempre existirá la posibilidad de que existan terceros que busquen manipular a dichas personas al conocer su identidad, como puede ser el caso de que la competencia busque influenciar a una persona para realizar un trabajo deshonesto comprometiendo la red desde su interior. (Binance Academy, 2020).

Dentro de este modelo también existen variaciones que se utilizan según la necesidad de la aplicación del Blockchain como puede ser Hyperledger o Ripple que son basadas principalmente en la Prueba de Autoridad, con algunas variaciones como puede ser en los procesos que realizan los cuales pueden llegar a ser más iterativos. (Prusty, 2020).

3.4 Prueba de Quemado (PoB)

Con todo el avance tecnológico con respecto a lo que son las criptomonedas y la tecnología de Blockchain es inevitable que se busque siempre corregir los fallos de los modelos ya existentes y mostrar así una nueva idea para implementar la cual solucione todas las fallas dando mejores resultados a la final, sin embargo es imposible crear un sistema perfecto, ya que al igual que el avance tecnológico en cuando a seguridad avanza siempre existirá un tercero que busque sacar provecho de manera ilegal de estos medios.

Este tipo de modelo fue presentado por Lain Stewart el cual mostro principalmente su invento de Prueba de Quemado mencionando analogías con respecto a los algoritmos predecesores. Uno de ellos puede ser que para este caso de tecnología lo que busca es que los mineros “quemen” sus monedas y que realicen compras de plataformas de minerías virtuales las cuales se encargaran de extraer nuevos bloques. Dando como tal a que en el caso de “quemar” una gran cantidad de monedas se pueda acceder a una plataforma minera mucho mayor. (Bit2me Academy, 2020).

Como se menciona en un inicio el proceso que realiza la Prueba de Quemado no tiene nada que ver con respecto a la minería para poder obtener nuevos tipos de criptomonedas. Sino que en realidad lo que se busque que sea posible quemar algunos tokens ya nativos o alguna alternativa similar para poder ganar un permiso para poder participar.

El funcionamiento de este modelo como tal es algo particular, ya que se busca que los mineros deben realizar el envío de las criptomonedas hacia una dirección que sea publica y completamente verificable. Este tipo de dirección se la puede

definir como dirección comedora en español, en la cual una vez ingresen no podrán volver a ser recuperadas de ninguna manera, similar a como si se realizara una inversión y a mayor sea la cantidad que se quemen mayor será la recompensa que puede obtener el minero. (Bit2me Academy, 2020).

Este proceso es principalmente para validar el compromiso que tiene un usuario con la red de la cual será participe, siendo en este caso similar a los protocolos que se utilizan en Prueba de Trabajo, variando que se invierte en tokens mas no en equipos costosos.

De esta manera se eliminaría el problema que se tenía en PoW al momento de querer realizar el conocido ataque del 51%. Después de todo para poder realizar este ataque el usuario tercero debería primero invertir en tokens para poder comprar más módulos y en el caso de ser identificado perdería todo lo invertido sin posibilidad de recuperarlo dando como tal un riesgo increíblemente grande para intentarlo.

A pesar de ser muy similar a PoW existen varias ventajas que puede brindar este tipo de modelo, como pueden ser:

- No se necesita un gasto excesivo al momento de necesitar energía o equipos computacionales específicos para el trabajo al brindar una solución más amigable y sostenible con el ambiente.
- Al invertir en el quemado de las monedas o tokens de manera virtual se elimina la necesidad de hardware especializado o incluso eliminando la aparición de compañías que centralicen el proceso.
- Al buscar una inversión para los participantes se llega a obtener un comportamiento honesto y confiable por parte de los usuarios al poner en juego su dinero real.
- Al utilizar protocolos de inversión se mantiene una estabilidad al hablar de los precios de la moneda.
- Se promueve la distribución de tokens nuevos de manera descentralizada y a su vez justa.

Sin embargo, no todo puede ser beneficios como ya mencionamos debido a que al requerir de tokens ya disponibles se pueden presentar los siguientes inconvenientes:

- Al usar tokens existentes es posible que estos provengan de modelos como Prueba de Trabajo haciéndolo un algoritmo ya no tan amigable con el medio.
- Como son transacciones de inversión la verificación que se tiene para cada uno de los mineros con los módulos de minería comprados toma un mayor tiempo en comparación a PoW.
- Al ser un proceso de inversión no existe total garantía de que los participantes recuperen su dinero en el caso de que no funcione del todo bien la red de Blockchain.
- Al tener una posibilidad de compra mayor al invertir más en tokens en un inicio puede llegar a tener gran control en las transacciones quienes más invierten.

4. Análisis de Resultados

Luego de todo lo estudiado con respecto al Blockchain como a los dispositivos de IoT podemos denotar que existen varias posibilidades para poder aplicar y juntar las características de ambos para brindar el mayor número de beneficios en conjunto. De tal modo que dentro de este apartado se pondrán en ejemplo algunas de las posibles aplicaciones que podrían tener y así tener un sistema seguro para el envío de información a través de este tipo de redes de bloques.

Como ya sabemos al hablar del Internet de las cosas podemos nombran un sinfín de posibilidades para usarlo, estas principalmente para beneficio y aumento de productividad en el tiempo o realización de acciones repetitivas, sin embargo, a pesar de todas las medidas de seguridad que se intenten implementar siempre existirá una brecha el cual puede funcionar como punto de ataque dando como resultado uno de los componentes más desafiantes de esta tecnología.

Para este punto como se recordara existen varios puntos de ataque para los dispositivos IoT como se mencionaron en capítulos anteriores que pueden venir de algo sencillo como una mala implementación de estos equipos como a un tema más complicado como los estándares existentes que estos utilizan y estos problemas se harán cada vez más grandes con el aumento del tiempo, pero como se vio el Blockchain es un método de cifrado que puede ser utilizado en una variedad de casos buscando innovar todo tipo de negocios o empresas a la vez que se camina de la mano con la seguridad de la información que se transmite.

Pero para plantear la principal incógnita del porque buscar un modelo que una estos dos tipos de tecnología deberemos tener en cuenta todos los beneficios que estas traen y buscar así brindar posibles soluciones que solventen las falencias de ambas.

Uno de los problemas más grandes en la actualidad de los exosistemas que trabajan con algunos dispositivos IoT es que trabajan de manera centralizada o incluso por medio de intermediarios, estos modelos son conocidos normalmente como cliente/servidor. (Banafa, 2017). Los cuales buscan que los dispositivos que están conectados a una red se deban identificar y autenticar con servidores, ya sean estos físicos o dentro de la nube, los cuales poseen gran capacidad de procesamiento como de almacenamiento. Y en cuanto a las conexiones que estos equipos tienen deben realizarse por medio del internet incluso si estos dispositivos se encuentran muy cerca uno del otro.

A pesar de que estos modelos cliente/servidor han funcionado durante décadas y seguirán siendo utilizados a futuro buscando implementar redes IoT no significa que sea una opción del todo viable, ya que a pesar de que se incluyan estas tecnologías únicamente han sido utilizadas a pequeña escala y como avanza la tecnología no será suficiente para complacer las necesidades del futuro de estos dispositivos.

Las soluciones que se muestran en el mercado en la actualidad llegan a alcanzar costos muy elevados al tratar con la infraestructura necesaria sin contar si quiera con los gastos que se deberán incluir a futuro para el mantenimiento de las nubes

que se utilizaran dentro de este entorno, o en otro caso los servidores y equipos de red físicos que se requieran para mantener a flote estos dispositivos. También hay que tener en cuenta que mientras más dispositivos se busque implementar dentro de la red se tendrán más conexiones entre ellos y la comunicación que deberán mantener entre estos aumentara notablemente el costo final para que los servidores los mantengan. Incluso si se llegara a obtener proveedores conocidos que brinden descuentos superando hasta cierto punto el factor económico y buscar capacitaciones para evitar contratos innecesarios para la implementación dentro de una red, los servidores que se tengan seguirán siendo un problema a la larga al convertirse en un cuello de botella al tener tantos dispositivos.

Es aquí en donde entran algunos beneficios que puede traer Blockchain como seria desde un inicio plantear un modelo en el cual se tenga un enfoque descentralizado para aplicar este tipo de redes de IoT. Al buscar tener un nuevo modelo estandarizado para lo que son las comunicaciones que se tendrán entre todos los dispositivos interconectados a la vez que procesar todas las transacciones que estos tendrían seria notable y de manera inmediata la reducción de costos que se tendrían. A la vez que aumentaría la productividad que podrían llegar a tener una empresa al no tener que recurrir con costos y tiempos de instalación y mantenimiento como se tendrían al tener un centro de datos centralizados, esto principalmente a que las necesidades computacionales que tengan los dispositivos IoT serian distribuidos por la red y almacenados a su vez entre miles de equipos que conformarían su red. (Banafa, 2017). Este tipo de implementación a su vez corregiría el problema que se tendría en el caso de que un solo nodo colapse y este a su vez afecte en consecuencia a toda la red.

Pero para ello tendríamos el siguiente problema en estos equipos que es el realizar las conexiones que se tendrán entre los dispositivos proporcionando un nuevo desafío en cuanto a la seguridad y como se mencionó en anteriores capítulos cuando se trata de redes con equipos IoT no solo se busca proteger los datos confidenciales.

Estos tipos de modelos que se deben plantear deben proponer una nueva manera de proteger la privacidad de la información a la vez que proporcionar un nivel alto de confiabilidad de las redes de IoT y finalmente con ellos proporcionar algún tipo de validación o consenso para todas las transacciones que se tengan para evitar toda posibilidad de robo o algún tipo de suplantación de identidad, el cual era uno de los beneficios que se tenían en los modelos de Blockchain. (Banafa, 2017).

Para lo cual hay que plantear de primera mano una un modelo que permita evitar las redes tradicionales de IoT que poseen un control totalmente centralizado teniendo como tales algunas funciones principales a cumplir, las cuales son:

- Poder tener mensajes de igual a igual
- Disponer de transacciones de archivos de manera distribuida.
- Que se tenga total coordinación con los dispositivos IoT que son autónomos.

Gracias a todos los beneficios que con lleva la tecnología de IoT podríamos asimilarlo a como si fuera un libro contable, el cual no puede ser manipulado por ningún tercero y únicamente puede acceder a la información cierto número de personas las cuales manejan los datos, a su vez tenemos la oportunidad de que este libro se encuentre totalmente distribuido evitando así un posible ataque de denegación de servicio y finalmente evitando el robo de información al tener diferentes hilos que manejan las transacciones es prácticamente imposible corromper toda la estructura de una red basado en una cadena de bloques para los dispositivos IoT.

Por lo cual podemos decir que las capacidades que brinda la tecnología de Blockchain lo convierten en un componente principal e ideal para poder funcionar con las futuras implementaciones que se deseen con IoT.

Uno de los beneficios que trae consigo al querer aplicar la tecnología de Blockchain dentro de una red de IoT, es que la cadena de bloques como tal puede manejar un registro cifrado e inmutable que pueden contener los datos de los dispositivos inteligentes como puede ser la información que comparten o la

historia que conllevan estos. (Banafa, 2017). Permitiendo una característica fundamental la cual es el trabajo autónomo de estos tipos de dispositivos inteligentes sin tener ningún intermediario que los controle de manera centralizada.

Como puede ser el caso del aprovechamiento de las cadenas de bloques en algunos modelos de IoT en los cuales se busque implementar un tipo de mensajería segura y sin confianza, es decir sin la necesidad de verificación de los equipos cada cierto tiempo al pertenecer a la red privada. Estos tipos de modelos se pueden implementar para que cuando dichos dispositivos deseen intercambiar mensajes esta comunicación se trate de manera similar a como si fuera una transacción financiera normal dentro de una red de criptomonedas, con ello estos dispositivos aprovecharían al máximo los contratos inteligentes creados por la red y a la final la comunicación seria transformada de manera que funcione acorde al modelo en el cual se implementó la red IoT. (Banafa, 2017).

Pero para elegir el tipo de tecnología de Blockchain que se quiere usar debemos tener en cuenta principalmente el modelo de IoT al cual será aplicado, por lo cual algunas de las características que podemos tener en cuenta en la revisión del modelo pueden ser las siguientes.

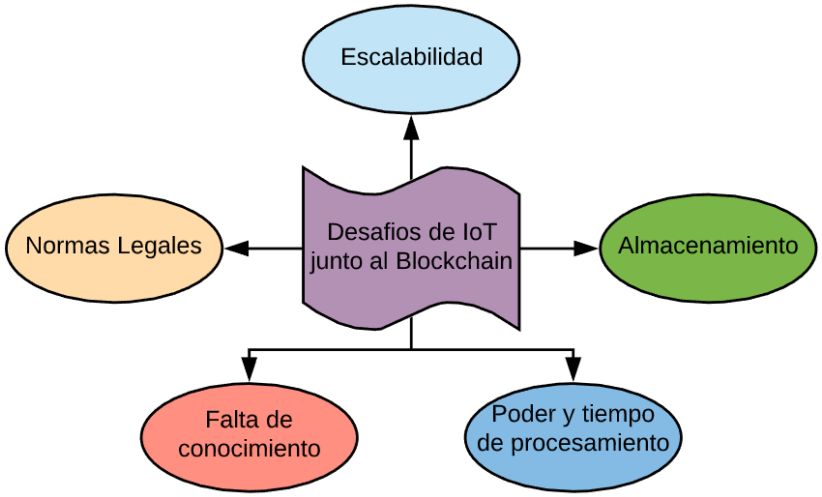

Figura 6. Desafíos de IoT frente al Blockchain

Hay que tener en claro que a pesar de ser un sistema de seguridad innovador y con ello más actualizado siempre se tendrán algunos defectos como cualquier otro modelo de seguridad y se deberá plantear diferentes opciones a seguir en el caso de que suceda cualquier imprevisto para poder allanar una posible falla en el modelo y lograr así disminuir el impacto que podría tener una empresa o solución.

- Los problemas con respecto a la escalabilidad pueden llegar a cambiar todo el punto de vista de lo que se desea, ya que si se aplica con una variedad demasiado extensa de dispositivos será necesario recurrir a la centralización de equipo poniendo en sí, el cual sería un problema a futuro para las criptomonedas debido a que podrían devaluarse al necesitar un trabajo mayor de uno de los nodos de la red.

- En cuanto al almacenamiento a pesar de que Blockchain busca eliminar la necesidad de implementar un servidor centralizado para las transacciones entre los dispositivos de la red, sin embargo, es necesario tener un nodo principal dentro de la empresa o aplicación de IoT la cual tendrá la información de todos los nodos restantes y en algunos casos como pueden ser sensores poseen un almacenamiento muy limitado.

- En cuanto a los equipos se necesitarán algunos que realicen el cifrado de los datos que se envían por el resto de los dispositivos IoT que están dentro de la red de Blockchain, por lo cual el procesamiento principal para el cifrado dependerá del modelo de IoT que se haya aplicado. Otro de los problemas que se deberán tener en cuenta es que no todos los dispositivos serán compatibles con los mismos algoritmos de cifrado o incluso que funcionen a una velocidad uniforme en la red.

- El problema con respecto al conocimiento es muy sencillo de entender, ya que al ser un modelo innovador el cual se quiere aplicar dentro de las redes se deberán realizar capacitaciones al personal que ya se tenga o

contratar nuevas personas a ello se le agregan diferentes equipos de diferentes proveedores y darían como tal un desafío bastante complicado.

- Finalmente, en cuando a la parte legal los dispositivos IoT avanzan de manera tan rápida que no se puede crear una normativa base para todos los dispositivos que se podrían crear con el paso del tiempo, mientras que el Blockchain al ser una tecnología disruptiva se busca que no sea aceptada de manera sencilla para no cambiar una estructura que lleva trabajándose durante siglos.

A pesar de que los dispositivos no serán de un mismo desarrollador se tiene que intentar realizar algún tipo de solución para que estos trabajen en conjunto, gracias a los protocolos como puede ser ethernet puede llegar a formarse una correcta coordinación y conectividad para cada una de las piezas que sean parte de la red. Una parte esencial es que todos los dispositivos trabajen en conjunto y sin problema alguno, a pesar de que sea un problema en cuanto al costo y la dificultad que se tenga para aplicarlos, ya que será lo mejor para el modelo a aplicar. (Banafa, 2017).

Existen algunos consejos que se pueden seguir para poder implementar un modelo óptimo para redes de IoT, basándose principalmente en opciones que agreguen un plus para la empresa entre esas opciones pueden ser las siguientes:

- Una plataforma que pueda adquirir y administrar datos de manera totalmente segura, que permita la escalabilidad y esté basada en estándares previamente creados.

- Buscar la integración y protección de los datos para poder reducir los costos de implementación a la vez que los costos para inversiones futuras.

- Analizar de primera mano los datos que se van a tratar para excluir los datos que o van a ser necesarios o no agreguen valor en la red.

Gracias a todos los modelos que han ido apareciendo con el tiempo es posible tomar la mejor opción para reducir costos y tener un modelo funcional, en un inicio evitar la centralización era prácticamente imposible al solo tener el modelo de Prueba de Trabajo, pero con los avanzas ahora podemos asegurarnos que la centralización ya no es un problema si se tienen las consideraciones pertinentes.

Como se mencionó este proyecto se realizó con el fin de descubrir algunos métodos de Blockchain aplicados dentro de los dispositivos IoT para poder preservar y asegurar los datos de manera efectiva, si se considera esta premisa podemos partir de lo que es como tal el concepto de autenticación el cual lo podemos definir como el proceso que permite como tal a un usuario el permiso para acceder a ciertos servicios o información verificando sus datos y confirmando la identidad del solicitante. (Balmaseda, 2018). Esto por lo general es implementado por el proveedor que ofrece los servicios el cual requerirá las credenciales para autenticarlas.

Lo que se espera es que a futuro con ayuda de la tecnología de Blockchain el enfoque que se tiene como tal de solicitar a alguien para ello desaparezca y como tal los modelos lleguen a descentralizarse, dando como resultado que toda la gestión y el control que se requiera para las credenciales como tal quede distribuido dentro de la propia cadena de bloques, dando una mayor seguridad a los datos que se transmiten por el funcionamiento de algoritmos criptográficos que posee Blockchain haciendo una red más confiable.

4.1 Solución N.1: Encriptar Llave Pública

Es posible considerar a las credenciales como entidades que serán parte en esencia de los datos que se envíen dentro de la cadena de bloques y esto sería verificados por todos los nodos participes con la ayuda de algoritmos para firmas digitales, como puede ser el caso de ECDSA o RSA que son capaces de realizar una conexión entre la clave publica que tendrían y los datos que se estarían

transmitiendo por la red, enviando como tal una clave privada al propietario dueño de la identidad y logrando así tener el permiso para firmar la autorización para el envío. Dentro de una aplicación web podríamos verlo como el portal que se suele tener para iniciar sesión para poder acceder a un servicio una vez validados los datos ingresados, solo que para este caso se buscaría tener un servidor descentralizado.

Dentro de los entornos que se utilizan en Blockchain existen flujos de igual manera para la autenticación que por lo general suelen ser genéricos y están principalmente basados en lo que se llama el Handshake, pero más enfocado a los bloques como tal.

Este proceso se realiza con el objetivo de entablar una comunicación con confianza entre los dispositivos, de tal manera que no se requieran intermediaros para el intercambio de información privada dentro de la red o la identidad que se utiliza en la misma.

En comparación a los tradicionales inicios de sesión que se suelen ver dentro de estos tipos de modelos no se requiere una contraseña como tal que se enviara al servidor principal, sino que se utilizará en vez de ello una aplicación que se encuentre protegida de tal manera que se envíe algún tipo de formulario para identificar el usuario como puede ser el caso de un código QR para comprobar la solicitud de conexión que desea el nodo y una vez confirmado enviarlo como autenticación. (Balmaseda, 2018).

El problema que se presentaría para estos casos es verificar que la aplicación que se está utilizando para el proceso de autenticación sea legitima y garantizar de tal manera que no acceda un tercero que busque ingresar a la red, a su vez también se tiene que comprobar que la respuesta que se tiene por medio de la aplicación también sea legitima para que no se realice una conexión falsa con otra persona o grupo de personas.

Este tipo de verificación iría de la mano con lo que es la criptografía de la clave pública la cual se basara principalmente en lo que son los certificados digitales, dando la posibilidad de firmar una solicitud que se enviara por la red y

verificándola públicamente dentro de la cadena de bloques formada por Blockchain, este tipo de proceso sería el cual suplantaría al intermediario dentro de la transacción. Por otra parte, al momento en el que el usuario que es dueño del nodo verifica una solicitud por medio de la aplicación que tenga instalada esta también será verificada con ayuda de la clave publica registrándolo como un nodo descentralizado parte de la cadena.

Para este proceso es posible utilizar lo que son los certificados X.509 el cual es un estándar creado por la Sector de Normalización de las Telecomunicaciones de la ITU. Este tipo de estándar va dirigido principalmente para la encriptación de claves públicas, realiza autenticación en directorios basándose en definiciones de certificados digitales que utilizan en esencia protocolos de internet, como por ejemplo TLS, entre otros. (Balmaseda, 2018).

En cuanto a los certificados claves podemos referirnos a ellos como aquellas acciones que son capaces de gestionar la información que lleva la misma y realizan procesos similares a la emisión, verificación, actualización, entre otros, pero el principal uso que se le daría dentro de la red de Blockchain seria para el manejo de claves.

Por medio de esta opción es posible realizar varios seguimientos tanto a equipos físicos como podrían ser los dispositivos IoT como a software como tal las cuales serían las aplicaciones que se utilizarían para la autenticación de los nodos.

Una vez sea aplicada esta opción como algoritmo es posible tener varias ventajas, e incluso llegar a aprovechar de terceros conocidos por el aplicante al tener la oportunidad de vincular identidades. Entre algunas de las opciones que se tienen al aplicar el algoritmo estarían:

- Permite mantener un registro de todas las solicitudes de los certificados enviados a su vez que estos son autenticados mediante su identidad en el nodo.
- Es posible generar pares de claves conocido también como criptografía asimétrica.
- Permite la total confidencialidad con las claves privadas que se envían.

- Verifica la vinculación entre el usuario o nodo y su clave pública.

Dentro de esta nueva identidad que tendrán los nodos la verificación que se tiene de estas ya no tienen que ver con una entidad centralizada que los controle, sino que los mismos usuarios junto a la red de bloques son los que se autentican de manera automática, haciéndolo un proceso totalmente descentralizado.

A estas nuevas identidades digitales que obtendrán los participantes de dichos nodos es posible nombrarla como entidad soberana y estas son generadas por el sistema digital y a su vez son cifradas, esta identidad tiene la posibilidad de almacenar datos de manera segura que son controlados totalmente por el usuario, por lo cual toda la identificación de los datos recae sobre ellos mismos permitiéndoles ser la autoridad máxima en el caso de ser el emisor a la vez que le permite controlar la clave privada del nodo, con ello solo los datos relevantes y que el usuario requiera transmitir serán enviados por la red, con Blockchain no cualquiera podrá hacer esto debido a que el usuario deberá probar antes de añadir un bloque su identidad y demostrar como tal que es dueño de ese nodo. (Balmaseda, 2018).

Este tipo de aplicaciones es posible realizarlas con la ayuda de código libre o guías que pueden ser encontradas por Microsoft, debido a que una de las opciones de aplicar este algoritmo puede ser mediante el centro de seguridad que posee Microsoft en Azure. Para ello se necesitaría la herramienta conocida como OpenSSL la cual posee código abierto y es accesible de manera local por un equipo Windows, ya en el caso en que una empresa o entidad más grande desee aplicar esto para su trabajo diario ya será necesario recurrir en gastos para certificados.

Con la aplicación ya instalada será sencillo crear una nueva autoridad para que se le permita autenticar por medio de una certificación un centro de dispositivos IoT.

Gracias a la facilidad que se ha tenido con las aplicaciones de Microsoft el realizar este proceso no conlleva tanta complejidad ya que únicamente será

necesario ingresar a las opciones de configuración y luego de ello se tendrá a la vez una opción de certificados, como es de costumbre Microsoft nos ira guiando en la creación y únicamente será necesario ir añadiendo los campos y presionar la opción siguiente hasta llegar a tenerlo creado.

A pesar de que se generó el certificado este aparecerá con un estado de que no ha sido verificado para ello únicamente deberemos modificar lo que es el certificado y generar un código que lo verifique como tal. Una vez se tenga dicho código es posible utilizarlo para validar el nodo que es dueño de dicho certificado. (Microsoft, 2019).

Cuando ya se verifico el código el proceso se deberá continuar con la firma para la verificación, esto se realizará por medio de la clave privada que se creó con el algoritmo x.509.

Luego de que creemos el certificado deberemos crear un dispositivo de IoT dentro del centro para poder manejarlo con esta autenticación, dentro de las mismas configuraciones existe el apartado para crear dispositivos.

Cuando ya tengamos tanto el dispositivo como la certificación pasaremos a firmarlo juntando estos dos campos. Según como avance un dispositivo este se deberá ir validando con la creación de un certificado intermedio dentro de la cadena, teniendo como resultado una cadena de certificados. Estos dispositivos validados es posible generarlos o simularlos mediante código en C# estos se verán como dispositivos autenticados dentro del centro de IoT.

4.2 Solución N.2: Basado en autenticación por tokens

Para este caso es posible aplicar mecanismos que mediante evaluaciones de presencia del usuario se establezca una seguridad continua dentro de la red de IoT creando una zona segura que no necesita intervención del usuario. Cada interacción que pueda tener un usuario será representada como una transacción la cual será almacenada dentro de la cadena de bloques.

Sin embargo, para que pueda existir una interacción de un usuario y ser tomada como legitima deberá ser verificada, para ello es necesario un mecanismo que

controle estas transacciones y evitar así los terceros que no estén autorizados a ingresar a la red, para lo cual será necesario la creación de un token. Estos tokens serán generados automáticamente según la necesidad de enviar información.

Actualmente existen tantas vulnerabilidades debido a que los procesos de la creación de la infraestructura que se utiliza son realizados manualmente y las seguridades que se implementan dejan muchos puntos de entrada para terceros por lo cual los sistemas de IoT se vuelven muy vulnerables a diferentes ataques.

Debido a los avances tecnológico es necesario que la participación de todos intermediarios de los equipos de IoT, se trabaje de manera automatizada para así poder crear un entorno que prevenga futuros problemas de seguridad y que no requiera tener confianza entre personas.

Gracias al funcionamiento que tiene Blockchain es posible aportar inmutabilidad y mantener esos datos distribuidos dando una mayor legitimidad a las transacciones o interacciones que tienen todos los dispositivos de IoT entre sí. Todas las interacciones que se realicen entre los dispositivos deberán ser almacenadas como si fueran una transacción esto principalmente para poder evitar que existan interacciones de personas sospechosas. (Agrawal, 2018).

Para poder resolver es posible crear tokens criptográficos para mantener la seguridad continua dentro de la red y estas interacciones que tendrán los equipos pueden determinar los movimientos que realizan, la transferencia de la información que han recolectado, la actividad que está realizando un usuario con ese equipo, entre otros.

Para poder centrarnos en la seguridad es posible aplicar lo que son las contraseñas de un solo uso, o preguntas de seguridad que se limitan a un solo funcionamiento. Pero para el caso de verificar que una ruta por la cual son enviadas es segura es posible que antes de ingresar las credenciales la identidad del usuario exista una mayor confianza con la identidad.

Este método puede ser aplicado con la creación de un similar a una base de datos para almacenar las interacciones que tiene un dispositivo o usuario por

medio de la cadena de bloques, una opción para esto puede el uso del software brindado por Hyperledger Fabric.

Gracias a que todas estas interacciones son almacenadas como transacciones es posible definir una secuencia y así poder ver un posible rastro de las actividades que realiza un usuario o cierto dispositivo. Gracias a Blockchain el sistema que se implementa de IoT no estará comprometido si existe un solo único punto de falla debido a la descentralización en el cual se aplica.

A pesar de que todos los nodos están interactuando autónomamente es importante que exista un nodo central o un centro de IoT el cual maneje de alguna manera todos estos dispositivos logrando que cada uno de los equipos se maneje sin mayores restricciones.

Es importante decir que en el caso de que se detecte algún tipo de acción sospechosa no se generara el token para agregar el bloque dentro de las cadenas facilitando los envíos de información sin interrupciones entre las zonas ya verificadas.

Como ya se mencionó la zona creada para los dispositivos IoT necesitan una supervisión para poder controlar a todos los usuarios, por lo cual es posible crear topologías para poder establecer conexiones entre los diferentes nodos o las múltiples zonas estas se mantendrán como reglas para todo el resto de los nodos ya sean nuevos o antiguos. (Agrawal, 2018). Con ello un ejemplo para poder validar el funcionamiento sería el siguiente.

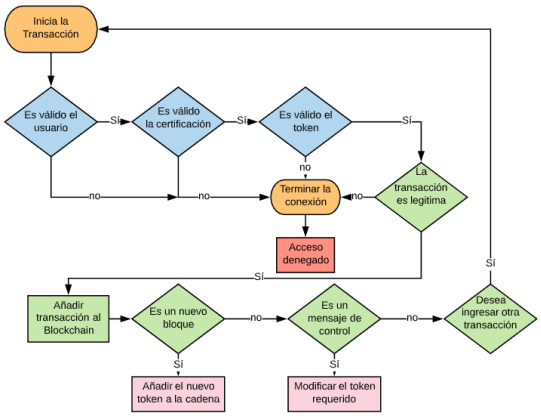

Figura 7. Opción modelo de funcionamiento

4.3 Solución N.3: Utilización de Hyperledger

Dentro de esta solución es posible utilizar las algunas de las soluciones que nos brinda Hyperledger y optimizarlas con los equipos que se requieran utilizar dentro de la red. Como tal podemos decir que Hyperledger es una colaboración de varias personas y organizaciones para poder brindar un open source principalmente dirigido al avance tecnológico en lo que refiere el Blockchain, llegando a si a las industrias de todo el mundo de una manera más sencilla.

Esta idea ya es considerada con un apoyo global por las empresas y su principal pilar fue la Fundación Linux, dentro de estas soluciones podemos encontrar un sinfín de opciones para poder utilizar como pueden ser para temas de Finanzas, mejoras tecnológicas, fabricación de dispositivos y la que tomaremos en cuenta la cual es la aplicación para el internet de las cosas.

Una parte para denotar de estas opciones es que debemos separarlas de lo que se tiene de manera global como idea de lo que es el Blockchain, ya que como tal Hyperledger no hace referencia a lo que es el Bitcoin como tal ni a ningún tipo de criptomoneda creada por otras opciones, sin embargo, si está impulsada por la definición y funcionamiento de una cadena de bloques. Esto principalmente para evitar los problemas que traerían consigo el uso de una moneda al no poder ser utilizada de manera global. (IBM, 2020).

De esta manera separamos el problema que trae el uso de las criptomonedas debido a que todas las personas únicamente interesadas en sacar una ganancia se eliminan del trabajo y se apuesta principalmente en mejorar los posibles servicios que se pueden brindar en un open source.

Existen varias opciones para escoger al momento de utilizar lo que es Hyperledger las cuales serán divididas según el objetivo que para el cual se va a aplicar este tipo de tecnología, por un lado tenemos diferentes Frameworks para trabajar como puede ser Fabric, Burrow, Indy, entre otros, y cada uno de ellos fue creado o impulsado por una idea distinta la cual nos hará más sencillo la elección de uno de ellos, ya que se puede seleccionar ideas semejantes a las cuales el proyecto se va a dirigir. (IBM, 2020).

Por otro lado, también deberemos escoger las herramientas que vamos a implementar dentro del proyecto como pueden ser, Faliper, Gello, Composer, entre otros. Esto será principalmente para definir la operabilidad que tendrá la red o como tal el funcionamiento que se incluirá como el manejo de nodos o manejos de librerías criptográficas. (IBM, 2020).

Para esta opción se utilizará lo que es el Hyperledge Fabric esto debido a que es una de las opciones más aceptadas por el mercado además de que este tipo de implementación es similar a un plug-and-play de lo que es el Blockchain, por lo cual es posible utilizarlo como pilar para desarrollar aplicaciones totalmente escalables y a su vez que posea varios permisos dándole un grado adicional de flexibilidad a la posible implementación. (IBM, 2020).

Una vez se tenga como tal Hyperledger Fabric podremos utilizar todas las características que esta puede brindar, sin embargo, se utilizará para la creación e implementación de tecnologías de registro distribuido, la cual será prácticamente una base de datos dentro del proyecto la cual pueda ser controlada por varios participantes conservando la característica principal de Blockchain la cual es que esta no esté centralizada. Esta aplicación da una gran ventaja, ya que similar a las otras opciones de Blockchain no se tiene una autoridad principal que verifique o acepte las cadenas que se van a agregar, eliminando la posibilidad de que exista algún tipo de fraude de la información que se va a enviar entre dispositivos.

Gracias a los servicios que nos puede brindar Hyperledger Fabric podremos crear diferentes nodos para poder así tener como tal nuestra red Blockchain descentralizada, los cuales serán:

- **Peers:** Estos nodos serán los encargados tanto de la simulación como el almacenamiento de las diferentes transacciones que se tendrán por parte del cliente. Toda la información que se genera en estos puntos será incluida dentro de los bloques del nodo.

- **Nodo Clientes:** Estos serán los nodos que envían o solicitan las transacciones a la red de Blockchain como tal, es decir serán nuestros dispositivos IoT. Estos al enviar la solicitud para la transacción requerida deberán esperar la confirmación de los nodos peers los cuales luego de simular la transacción decidirán si se aprueba o no el envío de esta. En el caso de que la transacción cumpla con las políticas aplicadas por el usuario será enviada al nodo orden el cual es el encargado de agregarlo a la cadena de bloques.

- **Nodo Orden:** Este nodo estará principalmente destinado al ordenamiento y entrega de las transacciones dentro de la red al destinatario peer al cual este definido o configurado desde un inicio. Este es uno de los nodos principales a establecer en la red debido a que se encargara de la concordancia que tengan las transacciones correspondientes a un tiempo definido.

Existen otros tipos de servicios que pueden ser instalados de ser requeridos, los cuales brindaran beneficios adicionales como puede ser la validación de que la información fue entregada u otros que brindaran tolerancia a fallos entre los diferentes nodos utilizados en la red, estos pueden ser los servicios de Kafka y Zookeeper.

5. Conclusiones

- Es importante denotar que como todas las tecnologías emergentes de hoy en día tienen sus fallas que se van actualizando con diferentes parches de seguridad buscando resolver las vulnerabilidades que se tengan, sin embargo, la mayor parte de la responsabilidad recae sobre el usuario al tener que actualizar todos los dispositivos.

- A pesar de conocer el significado de Blockchain no se tiene muy en claro al momento de hablar de él, ya que al momento de tocar el tema por lo general se lo asimila con los bitcoins centralizando el uso que se le puede dar a dicha tecnología y eliminando las posibilidades de futuras aplicaciones.

- Gracias a haber realizado un estudio de ambos temas es posible dar un modelo el cual puede beneficiar a futuras aplicaciones de estos y poder dar una solución aplicada en un ambiente real para una persona o grupo de personas.

6. Recomendaciones

- Al momento de querer buscar ya implementar un tipo de red de dispositivos de IoT hay que definir que equipos se utilizaran para poder hallar un uso común para que se los pueda utilizar evitando así sobrecargar de equipos dentro de una sola red.

- Gracias a que el Blockchain es una tecnología emergente y disruptiva es posible dar un nuevo camino a gran parte de las cosas ya existentes y con ello es posible encontrar gran parte de la información con respecto a dicha tecnología en un solo lugar, sin embargo, es importante diferenciar la información que va dirigida a un uso general y aquel que hace referencia únicamente a los bitcoins.

- Al momento de generar diferentes opciones como pueden ser modelos para poder utilizar de manera general la tecnología de Blockchain es importante que a pesar de ser una base la persona que busca ya implementar la opción tiene que buscar el centralizar las características aprovechables y buscar una mejora continua para el aprovechamiento de los equipos que disponga la red tomando en cuenta incluso el uso que puede llegar a tener tanto el software y hardware implementado.

Referencias

Abliz, M. (2015). *A Novel Puzzle-Based Framework for Mitigating Distributed Denial of Service Attacks Against Internet.* University of Pittsburgh.

Academy, B. (2008). *La Historia de Blockchain*. Recuperado el 10 de Febrero del 2020 de https://www.binance.vision/es/blockchain/history-of-blockchain

Academy, B. (2018). *¿Qué es la Prueba de Estaca (Proof of Stake)?* Recuperado el 25 de Abril del 2020 de https://academy.binance.com/es/blockchain/proof-of-stake-explained

Academy, B. (2020). *¿Qué es Proof of Burn (PoB)?* Recuperado el 25 de Abril del 2020 de https://academy.bit2me.com/que-es-proof-of-burn-pob/

Academy, B. (2020). *Proof of Authority Explained*. Recuperado el 20 de Abril del 2020 de https://academy.binance.com/blockchain/proof-of-authority-explained

Academy, B. (2020). *Qué es PoA (Proof of Authority – Prueba de Autoridad)*. Recuperado el 20 de Abril del 2020 de https://academy.bit2me.com/que-es-proof-of-authority-poa/

Academy, b. (2020). *Qué es Prueba de Trabajo*. Recuperado el 10 de Febrero del 2020 de https://academy.bit2me.com/que-es-proof-of-work-pow/

Agrawal, R., Verma, P., & Sonanis, R. (2018). Continuous Security in IoT Using Blockchain. *IEEE International*.

Albors, J. (2018). *Seguridad en dispositivos IoT*. Recuperado el 16 de Febrero del 2020 de https://www.welivesecurity.com/la-es/2018/07/25/seguridad-iot-a-tiempo-ganar-batalla/

Anzelmo, E., Caprio, D., & Van, K. (2011). *Internet of Things, Discussion.* Proceedings of 1st Berlin Symposium on Internet and Society.

Balmaseda, F. (2018). *Aseguramiento de Dispositivos IoT con Blockchain e Infrestructura de Clave Pública.* Madrid.

Banafa, A. (2015). *Internet de las cosas: Seguridad, privacidad y protección*. Recuperado el 16 de Febrero del 2020 de https://www.bbvaopenmind.com/tecnologia/mundo-digital/internet-de-las-cosas-seguridad-privacidad-y-proteccion/

Banafa, A. (2017). *Convergencia de IoT y Blockchain: beneficios y desafíos*. Recuperado el 2 de Marzo del 2020 de https://iot.ieee.org/newsletter/january-2017/iot-and-blockchain-convergence-benefits-and-challenges.html

BBVA. (2017). *De Alan Turing al 'ciberpunk': La historia del Blockchain*. Recuperado el 2 de Marzo del 2020 de https://www.bbva.com/en/alan-turing-cyberpunk-history-blockchain/

Champage, P. (2018). *El libro de Satoshi.* España: Publishing LLC.

CSIRT-CV. (2018). *Seguridad en internet de las cosas.* Valencia: Crative Commons.

Donohue, B. (2014). *Qué Es Un Hash Y Cómo Funciona*. Recuperado el 24 de Mayo del 2020 de https://latam.kaspersky.com/blog/que-es-un-hash-y-como-funciona/2806/

Fleisch, E. (2020). *What is the Internet of Things*. Recuperado el 16 de Febrero del 2020 de https://www.alexandria.unisg.ch/68983/1/AutoID%20-%20What%20is%20the%20Internet%20of%20Things%20-%20An%20Economic%20Perspective%20-%20E.%20Fleisch.pdf

Gracia, M. (2020). *IoT - Internet of Thing*. Recuperado el 16 de Febrero del 2020 de https://www2.deloitte.com/es/es/pages/technology/articles/IoT-internet-of-things.html

IBM. (Febrero de 2020). *Hyperledger Fabric: el marco flexible de blockchain que está cambiando el mundo empresarial*. Obtenido de https://www.ibm.com/blockchain/hyperledger

ITU. (2005). *The Internet of Things.* Unión Internacional de Telecomunicaciones.

Jiménez, D. (2019). *¿Cuantos algoritmos de consenso existen para las Blockchain?* Recuperado el 28 de Mayo del 2020 de https://es.cointelegraph.com/news/cuantos-algoritmos-de-consenso-existen-para-las-blockchain

Kranenburg, V. (2020). *IoT Challenges*. Recuperado el 16 de Febrero del 2020 de https://link.springer.com/article/10.1186/2192-1121-1-9

Meyer Gerben, F. K. (2020). *Intelligent Products: A survey: Computers in Industry.* Elsevier B.V.

Microsoft. (2019). *Configure la seguridad X.509 en su centro Azure IoT*. Recuperado el 6 de Mayo del 2020 de https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-security-x509-get-started

Novo, O. (2018). Blockchain Meets IoT: an Architecture for Scalable. *Journal of Internet of Things*.

Prusty, N. (2020). *¿Qué es el consenso de prueba de autoridad?* Recuperado el 27 de Mayo del 2020 de https://www.oreilly.com/library/view/building-blockchain-projects/9781787122147/827f4856-1b32-4a10-a53a-e02050f74a15.xhtml

Rodríguez, A. (2020). *Conoce que es la interoperailidad del IoT*. Recuperado el 18 de Mayo del 2020 de https://www.telcel.com/empresas/tendencias/notas/interoperabilidad-del-iot

Rojo, M. (2020). *Blockchain: Visión tecnológica*. Recuperado el 23 de Marzo del 2020 de https://www2.deloitte.com/es/es/pages/technology/articles/blockchain-vision-tecnologica.html

Society, I. (2015). *Internet Society*. Recuperado el 23 de Marzo del 2020 de https://www.internetsociety.org/wp-content/uploads/2017/09/report-InternetOfThings-20160817-es-1.pdf

Stallings, W. (2006). *Cryptography and Network Security: Principles and Practice.* New York: Prentice Hall Press.

Tar, A. (2019). *Qué es Prueba de trabajo o Proof of Work (PoW)*. Recuperado el 27 de Mayo del 2020 de https://es.cointelegraph.com/explained/proof-of-work-explained

Thales. (2019). *La seguridad del IoT*. Recuperado el 16 de Febrero del 2020 de https://www.thalesgroup.com/es/countries/americas/latin-america/dis/iot/seguridad-en-iot