Como citar este artículo: Y. I. L. Lucio, K. Márceles Villalba and S. A. Donado, "Adaptive Blockchain Technology for a Cybersecurity Framework in IIoT," in *IEEE Revista Iberoamericana de Tecnologias del Aprendizaje*, vol. 17, no. 2, pp. 178-184, May 2022, doi: 10.1109/RITA.2022.3166857.

Tecnología Blockchain adaptable para un framework de ciberseguridad en IIoT

Yeison LLante Lucio, Katerine Márceles Villalba, Siler Amador Donado

***Abstract*—This article presents the problem regarding the assurance of the information that circulates in the devices that are connected to the internet, due to the multiple threats to which they are exposed, running the risk of losing or leaking information; However, with the passage of time, new technologies are emerging that encourage organizations to maintain continuous improvement of their applications and tools, but at the same time the emergence of new technologies brings with it cybersecurity risks that organizations must face when carrying out an integration with them. Therefore, through the action research methodology, two phases were defined, one of them reviewing Blockchain technologies and the second comparing Blockchain technologies to finally determine the most adaptable technology to a cybersecurity Framework focused on IIoT, capable of managing the integrity of the information and achieving a consensus among all the nodes belonging to a certain network.**

***Index Terms*— Blockchain, Cyber-security, Framework, IoT.**

I. Introducción

En la actualidad la industria 4.0 tiene un gran impacto frente a la innovación de nuevas tecnologías que ayudan para que las personas puedan realizar tareas de un modo más sencillo y ágil de cara a esta oportunidad son muchas las organizaciones que han aprovechado todo el auge que han tenido los pilares de esta industria y en relación con estos se encuentra el internet de las cosas (IoT), el cual ha tomado un papel importante en la vida cotidiana de las personas logrando que el internet de las cosas con aplicaciones industriales (IIoT) se convirtiera en una adopción frecuente por parte de las empresas para la implementación de sus productos. En este sentido, el crecimiento que ha tenido (IIoT) ha sido muy amplio, 100 mil millones de conexiones IoT es una proyección que ha realizado la compañía Huawei para el año 2025 [1].

Lo anterior, es una gran noticia que da entender que cada vez más son las organizaciones y/o usuarios que estan adoptando esta tecnología; sin embargo, generan determinados riesgos de seguridad que colocan en peligro la información sensible que puedan recolectar los dispositivos, entre los riesgos más habituales a los que se expone un sistema IIoT están: la infiltración en redes internas, espionaje a través de los dispositivos, pérdida de información y de control sobre los dispositivos.

Normalmente las organizaciones toman medidas para aplacar o reducir los riesgos mencionados anteriormente, una de estas medidas implicaría hacer uso de CIDS (Collaborative Intrusion Detection System), que no son más que, distintos detectores de intrusos que comparten entre ellos información para ampliar un mayor rango de detección. No obstante, uno de los problemas que tiene los CIDS es la gestión de confianza entre los nodos; por lo tanto, si un nodo es comprometido o empieza a enviar información falsa, su nivel de confianza descenderá pudiendo llevarse a cabo distintas acciones, como, por ejemplo: introducir ese nodo en una blacklist [2]. Por un lado, otra vulnerabilidad latente ocurre en el transporte de los datos que recolectan dichos dispositivos, ya que el 98% del tráfico de dispositivos de IoT no está cifrado, lo que coloca en riesgo los datos personales y confidenciales en la red. Los atacantes que han superado con éxito la primera línea de defensa (con mayor frecuencia a través de ataques de phishing) han establecido el comando y control que pueden escuchar el tráfico de red no cifrado, recopilar información personal o confidencial y luego explotar esos datos para obtener ganancias por estar en sitios como la Dark Web [3], es por ello que la tecnología blockchain cobra fuerza, dado que consiste en asegurar la información avalando que no ha sido modificada durante su circulación; por consiguiente, una de sus principales ventajas es que con Blockchain se puede mejorar la comunicación entre los nodos de una red de dispositivos IIoT para que estos puedan compartir información que es importante para su consenso. Normalmente, los dispositivos IIoT están conectados mediante una red para que puedan enviar sus datos recolectados hacia internet, es aquí donde Blockchain toma un papel relevante, ya que es vital que estos dispositivos que son conocidos como nodos dentro de la red se puedan comunicar en caso de un posible ataque y así evitar que otros nodos de la red se vean afectados. De acuerdo a lo mencionado anteriormente, surge la necesidad de integrar la tecnología Blockchain para entornos IIoT y así poder mejorar el nivel de seguridad; por consiguiente, en este artículo se dará a conocer la selección de la tecnología Blockchain que más se adapte para un framework de ciberseguridad en IIoT, mediante el enfoque metodológico de la investigación acción, entendiendo ésta que utiliza una colección de datos de tipo cuantitativo, cualitativo o mixta y se centra en la solución de un problema específico y práctico [4], que en este caso en

Y. Isacc Llante Lucio, Facultad de Ingeniería, Institución Universitaria Colegio Mayor del Cauca, Carrera 7 N° 2-34 Edificio Bicentenario, 190003, Popayán- Cauca, Colombia(yeison.1266@unimayor.edu.co).

K. Márceles Villalba, Facultad de Ingeniería, Institución Universitaria Colegio Mayor del Cauca, Carrera 7 N° 2-34 Edificio Bicentenario, 190003, Popayán- Cauca, Colombia(kmarceles@unimayor.edu.co).

S. Amador Donado, Facultad de Ingeniería Electrónica y Telecomunicaciones, Universidad del Cauca, Carrera 2 #4N-140, 190003, Popayán- Cauca, Colombia (samador@unicauca.edu.co).

cuanto a lo específico es el abordar el problema que existe en lo que respecta el aseguramiento de la información que circula en los dispositivos conectados al IoT por lo que se requiere definir el tipo de tecnología Blockchain que permita gestionar integridad y en lo práctico el estudio del tipo de tecnología Blockchain que permita desplegarse en un Framwork de ciberseguridad.

II. CONCEPTUALIZACIONES

A. Ciberseguridad

La ciberseguridad se centra en establecer controles que permita salvaguardar las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques que pongan en riesgo la confidencialidad, integridad y disponibilidad [5]. La mayoría de los dispositivos electrónicos interactúan entre sí, ya sea directa e indirectamente a través de redes de datos o por medio de dispositivos de almacenamiento como por ejemplo: memorias USB que almacenan y transportan información de un dispositivo a otro, la ciberseguridad o seguridad de la información electrónica está encargada de proteger las redes de ordenadores de ataques maliciosos, mantener el software libre de amenazas, para así proteger la integridad de los datos tanto de una empresa o de una persona.

B. Blockchain

Blockchain es un registro de todas las transacciones que se empaquetan en bloques que los mineros luego tienen la función de verificar [6]. La tecnología Blockchain nace como soporte para las transacciones con Bitcoin. Desde sus inicios y hasta la actualidad Blockchain se utiliza en mayor parte en el ámbito de las criptomonedas, debido a la gran popularidad que ha tenido bitcoin; sin embargo, por debajo de todo lo relacionado con el tema de monedas digitales esta cadena de bloques (Blockchain) permite que esos activos puedan operar haciendo uso de libros de contabilidad descentralizados cuyo objetivo principal es mantener un registro de todas las transacciones que circulan por toda la red para que ese ecosistema funcione se tienen diferentes participantes como: los mineros cuyo papel es fundamental en las Blockchain de tipo públicas, ya que son los encargados de recolectar todas las transacciones que se encuentren pendientes y sumarlas a la red mediante la generación de un bloque. Para sumar un bloque a la red los mineros deben resolver un algoritmo matemático y el primero en encontrar esa solución pueden realizar dicha labor, para después obtener un beneficio económico.

El principal objetivo de Blockchain es garantizar que la información relacionada con las transacciones realizadas se mantenga en el tiempo totalmente inmutable logrando mantener la integridad de la información, pero además también busca quitar a los intermediarios, ya que en los sistemas centralizados tienen un determinado control sobre la información que almacenan. Si bien en sus inicios Blockchain tuvo un enfoque direccionado al ambiente de las finanzas, tiempo después se fueron conformando cadenas de bloques que ofrecían diferentes características hasta llegar al punto en el existen 3 tipos de Blockchain que se muestran a continuación.

- Blockchain pública

Este fue el primer tipo de Blockchain en existir, las cuales son de fácil acceso para cualquier usuario a través de internet un ejemplo de este tipo es Bitcoin y Ethereum. Este tipo de Blockchain posee medidas de seguridad para que actores maliciosos no les afecten y le permitan garantizar su correcto funcionamiento.

- Blockchain Privada

Una Blockchain privada, se distingue de una Blockchain pública, por no ser abierta al público, dado que solamente puede ser accedida a través de una invitación. Las Blockchain privadas son más recientes que las Blockchain públicas. Este tipo de Blockchain dependen de una unidad central que gestiona las acciones al interior de la misma. La unidad central es quien se encarga de dar acceso a los usuarios y verificar funciones y permisos dentro de la Blockchain [7]. Unos ejemplos de éstas son: Hyperledger-Fabric y Ethereum.

- Blockchain Híbrida

Este tipo de Blockchain esta compuesta entre las Blockchain públicas y las privadas. Busca aprovechar lo mejor de ambas tendencias. Una Blockchain híbrida, tiene una participación en la red de manera privada, en virtud de que el control a los recursos de la red es gestionado desde la unidad central, por lo que usuarios o nodos colaboran en el mantenimiento y seguridad de esta Blockchain; sin embargo, las transacciones son visibles para usuarios en todo el mundo y no necesariamente deben conocer el contenido de la Blockchain [8]. El libro de contabilidad es de acceso público, esto quiere decir que cualquier persona puede examinar bloque a bloque todo lo que ocurre en esta Blockchain.

C. IIoT

Con la llegada del internet de las cosas la industria percibió que se podía aprovechar esa tecnología en sus operaciones para ello surge el internet industrial de las cosas (IIoT). Se refiere a la estrecha relación entre la computación, redes y objetos físicos para la industria, en el cual los dispositivos están conectados en red para identificar, monitorizar y controlar el mundo físico para promover y gestionar el progreso de la industria [9]. La IIoT está cambiando el mundo de la industria en lo que se refiere a la automatización en sus procesos de fabricación pues los dispositivos o máquinas se pueden conectar y transferir datos entre sí, el IIoT busca la interacción de máquinas, sensores, personas y la computación en la nube, permitiendo comunicar e interactuar en tiempo real para monitorizar, controlar los procesos de fabricación, para mejorar la productividad y el desempeño de la maquinaria dentro de la industria.

D. Riesgo

El riesgo asociado a la seguridad de la información se define como “la posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad generando una pérdida o daño sobre un activo de información” [10]. El riesgo se compone de la amenaza y la vulnerabilidad, se puede referir también el concepto de riesgo a una ecuación donde sus variables incluyen la combinación de la probabilidad de ocurrencia de un incidente de seguridad.

E. Amenaza

Una amenaza se conceptualiza como la causa de un incidente no deseado, que puede provocar daños a un sistema o a la organización [10]. Una amenaza se caracteriza por aprovecharse de las vulnerabilidades para atentar contra la seguridad de un sistema de información, por lo que podría generar un efecto negativo sobre los activos de una organización.

F. Vulnerabilidad

La vulnerabilidad puede definirse como una debilidad de un activo o control que puede ser explotada por una o más amenazas [10], es una falencia en un sistema de información que puede llegar a poner en riesgo la confidencialidad, integridad y disponibilidad de la información, por lo que es necesario encontrarlas para gestionarlas.

III. TRABAJOS RELACIONADOS

Aseguramiento de Dispositivos IoT con Blockchain e Infraestructura de Clave Pública [11]. En este artículo se establece un entorno PKI (Infraestructura de clave pública) para realizar autenticación de dispositivos IoT de una forma segura haciendo uso de la Blockchain de Ethereum; también realizan un análisis de riesgo para identificar las mejoras obtenidas en términos de seguridad y para ello se establece una metodología de auditoría basada en riesgos que permitirá valorar los prototipos con el fin de revisar las mejoras resultantes en términos de seguridad.

IDS colaborativo basado en Blockchain [12]. Este artículo muestra el desarrollo de una Blockchain desde cero orientada a operar con IDS. Además, enseña las tecnologías utilizadas y la estructura del proyecto. Este trabajo resalta la forma en que desarrollan una red Blockchain desde cero pensada y diseñada para integrarse con el IDS SNORT, para el trabajo que se está desarrollando es importante tener en cuenta este tipo de consideraciones, ya que permite entender más a detalle el funcionamiento de una red Blockchain a nivel de implementación y cómo realizar una integración entre un IDS y una Blockchain. Por ese motivo este artículo, se toma como referencia principalmente por su integración de IDS junto a Blockchain.

Desarrollo de un sistema de trazabilidad en entornos IoT mediante Hyperledger [13]. Este proyecto abarca el desarrollo de una prueba de concepto (Proof of Concept - PoC-) para la implementación de Hyperledger-Fabric (HF) en el IoT. El propósito de esta fue la recopilación de eventos a través de sensores situados en una placa simple como la Raspberry Pi 3 (RPi) y la inclusión de incidencias en la Blockchain de HF. Del mismo modo, la información recopilada puede ser consumida en tiempo real mediante un sistema web. De este trabajo se destacan unas características interesantes como lo es el desarrollo de una Blockchain haciendo uso de tecnología Hyperledger y su integración con IoT, esto es de gran importancia para el presente proyecto, debido a que esta herramienta permite construir Blockchain muy completas que se adaptan perfecto a la Blockchain que se tiene planeado implementar, previo al estudio de éstas.

Intrusion detection system for the internet of things based on blockchain and multi-agent systems [14]. Esta investigación se centra en el diseño, implementación y prueba de un sistema de detección de intrusos que utiliza una estrategia de ubicación híbrida basada en un sistema multi-agente, Blockchain y algoritmos de aprendizaje profundo. El sistema consta de los siguientes módulos: recopilación de datos, gestión de datos, análisis y respuesta. Esta utiliza un conjunto de datos NSL-KDD del laboratorio de seguridad nacional. La presente investigación aporta al proyecto la implementación del sistema de detección de intrusos y su integración con algoritmos de aprendizaje profundo, ya que permite que se pueda entender de una forma más explícita el funcionamiento e integración de estas dos tecnologías, lo cual es de suma importancia para el desarrollo del framework propuesto.

IV. DESARROLLO METODOLÓGICO

Con el fin de establecer la tecnología Blockchain que más se adapte para un framework de ciberseguridad en IIoT se hace uso de la metodología de investigación acción [15], la cual consiste en unir la teoría con la práctica de tal forma que el investigador pueda sacar conclusiones acertadas sobre las acciones realizadas. Es por ello, que en esta ocasión el desarrollo de este trabajo se realizó a partir de dos fases, donde la primera se enfoca en hacer una búsqueda exhaustiva acerca de esta tecnología y la segunda en la determinación de la tecnología Blockchain más adecuada a partir de las necesidades y fortalezas, a continuación se describen las fases:

Fase 1: Revisión de las tecnologías Blockchain empleadas en los artículos clasificados como primarios.

Inicialmente se realizó una revisión sistemática general sobre las tecnologías que se encuentran involucradas en el framework que se plantea construir, esta revisión implicó efectuar búsquedas en bases de datos relacionadas con ciencias de la computación que permitan obtener artículos referentes con la temática planteada. En su totalidad se obtuvieron 201 artículos que fueron filtrados identificando cuántos de esos artículos se encontraban repetidos y cuales se consideraban más relevantes de acuerdo a su título, resumen y palabras clave. Teniendo en cuenta ese filtro inicial el listado de artículos se redujo a 67 considerados como artículos primarios que contienen en su interior información sobre tecnologías relacionadas que son importantes para la construcción del framework, como se puede evidenciar en la Tabla 1 se realizó una clasificación de artículos de acuerdo a cada tecnología.

TABLA 1
CLASIFICACIÓN POR TECNOLOGÍA

Tecnología	Cantidad
IoT	52
IDS	30
Blockchain	33
IA	28
Framework	22
Cloud	12

Ahora bien, como se menciona anteriormente la construcción de un framework puede involucrar a muchas tecnologías que para la revisión sistemática deben ser tenidas en cuenta; por lo tanto, partiendo del listado de artículos primarios se procede a clasificar cada uno de los artículos teniendo en cuenta la tecnología de la cual se quiere indagar más a detalle. Como se puede observar en la tabla 1, aplicando la clasificación por tecnología se obtienen que 33 de los artículos primarios tienen temáticas relacionadas con la tecnología Blockchain, 52 con estudios que abarcan el IoT, 30 artículos relacionados con IDS, 28 artículos que abarcan la temática de IA, 22 artículos que refieren a la construcción del framewok y finalmente 12 artículos que tocan aspectos de almacenamiento en Cloud(nube).

Dado a los resultados obtenidos por tecnología, se procede a revisar cada uno de los artículos identificados que abordan el tema relacionado de blockchain y a partir de esta revisión finalmente se obtiene un nuevo listado de artículos que mencionan una tecnología de Blockchain concretamente, como se puede observar en la tabla 2.

TABLA 2
LISTADO DE ARTÍCULOS QUE ABORDAN SOBRE TECNOLOGÍAS BLOCKCHAIN

#	Año publicación	Título del articulo u estudio	Autor(es)	Tecnologías Blockchain
1	2018	Aseguramiento de dispositivos IoT con Blockchain e infraestructura de clave pública	[6]	Ethereum
2	2018	Desarrollo de un sistema de trazabilidad en entornos IoT mediante Hyperledger	[12]	Hyperledger
3	2019	Secured Framework for IoT Using Blockchain	[16]	Ethereum
4	2020	Research on distributed blockchain-based privacy-preserving and data security framework in IoT	[14]	Hyperledger
5	2020	A Deep Blockchain Framework-enabled Collaborative Intrusion Detection for Protecting IoT and Cloud Networks	[17]	Ethereum
6	2019	A security framework for IoT authentication and authorization based on blockchain technology	[18]	Hyperledger
7	2019	A Blockchain Based Decentralized Authentication Framework for Resource Constrained IOT devices	[19]	Ethereum
8	2019	A Secure Framework for Communication in Internet of Things Application using Hyperledger based Blockchain	[20]	Hyperledger
9	2018	Intrusion Detector for Blockchain based IoT Networks	[21]	Ethereum
10	2019	Blockseciotnet: Blockchain-based decentralized security architecture for IoT network	[22]	Ethereum
11	2020	Utilizing Blockchain for Distributed Machine Learning based Intrusion Detection in Internet of Things	[23]	Ethereum
12	2020	Unification of Blockchain and Internet of Things (biot) requirements, working model, challenges and future directions	[24]	Ethereum, IOTA, Bitcoin, Hyperledger
13	2020	Bacs A Blockchain-based access control scheme in distributed internet of things	[25]	Ethereum
14	2020	Towards building a Blockchain framework for IoT	[26]	Ethereum, IOTA, Hyperledger

Posteriormente, cada uno de los artículos que se encuentran en la tabla 2, fueron revisados para obtener información relevante sobre cada una de las tecnologías de la cual trataba y así poder obtener características que permitieran realizar una caracterización de las tecnologías Blockchain mencionadas en esos artículos.

Fase 2: Comparar las tecnologías Blockchain encontradas

En esta fase lo primero que se realizó fue extraer todas las tecnologías Blockchain que mencionaban en el listado de artículos de la tabla 2, seguidamente realizar una caracterización de las mismas haciendo uso de características obtenidas a partir de la lectura de los artículos y de las necesidades que tiene el framework frente a esta tecnología. En esta caracterización se tuvieron en cuenta las siguientes Blockchain:

Ethereum: Es un proyecto de código abierto y desarrollado por la Ethereum Foundation. Es un conjunto de protocolos que integran una plataforma descentralizada que funciona bajo la tecnología Blockchain personalizada con una infraestructura global compartida que permite la programación y ejecución de aplicaciones autoejecutables con tiempo de actividad garantizando el 100%, sin interferencias de terceros y sin posibilidad de algún tipo de fraude interrupción o censura [6].

Hyperledger-Fabric: Se encuentra basado en el protocolo de consenso “Practical Byzantine Fault Tolerance (PBFT)” y es mantenido por el consorcio Linux Foundation, por lo cual es totalmente open source. Este proyecto hace uso de una arquitectura de cadena de bloques de alianza que puede confirmar información de bajo retraso, consumo de energía y costo de computación sin bifurcación de bloques cuando se implementan múltiples aplicaciones en el sistema IoT. Este tipo de arquitectura puede lograr verificación de la

información sin cobrar tarifa por transacciones realizadas entre los nodos de la red, lo cual es una gran ventaja ya que muchas Blockchain cobran por cada transacción realizada [14].

IOTA: Es un libro mayor distribuido enfocado directamente para IoT que utiliza un consenso llamado "Tangle", se basa en un grafo acíclico dirigido (DAG), donde los vértices representan intercambios y las bordes representan aprobaciones. Este consenso al estar enfocado para IoT no usa bloque para almacenar datos; en cambio, cada transacción es un bloque único. Para crear una transacción los nodos inicialmente firman la transacción y eligen dos transacciones anteriores al azar para aprobar. Cuando un nodo emite una nueva transacción, debe aprobar dos nodos anteriores, el nodo recién creado se llama entonces "tip", este nodo permanecerá como "sugerencia" hasta que un nodo recién creado lo apruebe [26].

Bitcoin: Este proyecto open source fue el primero en surgir y fue el que dió origen a la tecnología Blockchain y del cual muchas otras organizaciones tomaron como base para implementar sus propias Blockchain. Bitcoin fue desarrollada con el objetivo de implementar una moneda digital basada en el uso de cadenas de bloques para registrar las transacciones en una red totalmente descentralizada y así poder evitar la intervención de entidades centrales que supervisen y regulen las transacciones [6]. Bitcoin hace uso de mineros, quienes son los encargados de recolectar todas las transacciones y descifrar un algoritmo hash y poder sumar dichas transacciones a la cadena de bloques, para eso bitcoin hace uso del consenso proof of work (PoW), el cual tiene un alto costo computacional para los mineros que son los que reciben recompensas por ese costo computacional gastado.

V. RESULTADOS

A continuación, se presenta un análisis de resultados a partir de la información obtenida del ítem anterior.

En la tabla 3, se muestra la caracterización inicial de las tecnologías Blockchain que fueron determinadas como posibles candidatas para su implementación e integración con un framework de ciberseguridad en IIoT, para la selección se tuvieron en cuenta las características que hacen parte de necesidades identificadas para la construcción del framework propuesto.

En virtud, de que se pretende es seleccionar una tecnología Blockchain que mejor se artícule a las necesidades identificadas para la implementación del framework se debe tener en cuenta ciertos criterios de selección que permitan realizar una ponderación y a su vez llegar a la tecnología más apropiada; por ello en la tabla 4 se muestran los criterios de selección que se tuvieron presentes para realizar una caracterización de las tecnologías Blockchain que más sobresalen hoy en día. Estos criterios de selección se establecieron con base en características que hacen parte de las necesidades del framework que se requiere construir, por esa razón estas características se fueron generando a partir de la lectura y análisis de los artículos presentados en la tabla 2 y de la identificación de necesidades para la construcción del framework, por lo que se debe tener en cuenta el enfoque y las tecnologías que se van a utilizar por ejemplo: en este caso el framework esta direccionado hacia la ciberseguridad; de modo que, la confidencialidad de los datos es uno de los principales puntos que se deben tener muy presente.

Como se indica en la tabla 4, cada criterio de selección tiene valores cualitativos y cuantitativos, los cualitativos permiten identificar de forma clara si la tecnología cumple con determinada característica, por su parte los valores cuantitativos son de utilidad al momento de realizar una determinada ponderación, de manera que los valores cuantitativos son una representación numérica de la apreciación cualitativa, teniendo en cuenta una escala de 0 a 1, donde 0 es el valor más bajo; por tanto la característica no se estaría cumpliendo y su equivalencia cualitativa corresponde a No y 1 el valor mas alto; indicando que la característica se cumple en su totalidad por consiguiente su equivalencia cualitativa es Si.

TABLA 3
CARACTERIZACIÓN INICIAL DE LAS TECNOLOGÍAS BLOCKCHAINS

Características / Blockchain	Ethereum	Hyperledger-Fabric	IOTA	Bitcoin
Privada	Si	Si	No	No
Contratos inteligentes	Si	Si	No	No
Open source	Si	Si	No	Si
Datos confidenciales	No	Si	No	No
Autenticación e integridad	Si	Si	Si	Si
Gestión de claves	No	Si	No	No
Gestión de identificaciones	No	Si	No	No
Latencia de confirmación de transacción	15-20s	menor	60-3600s	600s

TABLA 4
CRITERIOS DE SELECCIÓN PARA LA TECNOLOGÍA BLOCKCHAIN

	Descripción	Característica	Valor cualitativo	Valor cuantitativo
1	Identifica el tipo de Blockchain	Privada	Si	1
			No	0
2	Determina si la tecnología Blockchain permite hacer uso de contratos inteligentes	Contratos inteligentes	Si	1
			No	0
3	Permite identificar si la tecnología es de código libre	Open source	Si	1
			No	0
4	Con esta característica se determina si los datos en el interior de la red se mantienen confidenciales	datos confidenciales	Si	1
			No	0
5	Identifica si la tecnología maneja autenticación y si se puede garantizar integridad de la información	Autenticación e integridad	Si	1
			No	0
6	Determina si la tecnología maneja		Si	1

	gestión de claves para el acceso a la red	Gestión de claves	No	0
7	Permite identificar si la tecnología permite realizar la gestión de identificaciones de los participantes de la red	Gestión de identificaciones	Si	1
			No	0
8	Permite identificar un tiempo aproximado de la latencia de confirmación de transacciones	Latencia de confirmación de transacción	60s<	1
			>60 && <=600s	0.5
			>600	0

En la tabla 5, se pueden observar los promedios obtenidos luego de hacer uso de los criterios de selección definidos previamente, como se puede visualizar la tecnología Blockchain que mejor resultó valorada y por ende se adapta más a las necesidades del framework a construir es Hyperledger-Fabric.

De acuerdo con [26] Hyperledger-Fabric es la plataforma más selecta, debido a su consenso conectable, la confidencialidad de los datos que es un punto importante a tener en cuenta cuando se utiliza tecnologías como IoT que por lo regular sus datos pueden llegar a ser muy sensibles, de manera que requieren de una infraestructura que permita salvaguardar esa integridad; así mismo, es de destacar que Hyperledger-Fabric pes el más utilizado, debido a el requisito mínimo de cálculo que tiene frente a otros en la actualidad.

Sin embargo, es relevante mencionar la segunda opción mejor valorada fue Ethereum, pero como se puede observar en la tabla 5, esta tecnología Blockchain tiene ciertas limitaciones en cuanto a la confidencialidad de los datos, dado que Ethereum desde sus inicios se consolidó como una Blockchain pública y que posteriormente fue incursionando en redes de tipo privadas, pero dada su naturaleza aún le falta tener en cuenta este tipo de características que permitan mantener ese nivel de confidencialidad de los datos.

TABLA 5
CARACTERIZACIÓN FINAL DE LAS TECNOLOGÍAS BLOCKCHAIN

Características / Blockchain	**Ethereum**	**Hyperledger-Fabric**	**IOTA**	**Bitcoin**
Privada	1	1	0	0
Contratos inteligentes	1	1	0	0
Open source	1	1	0	1
datos confidenciales	0	1	0	0
Autenticación e integridad	1	1	1	1
Gestión de claves	0	1	0	0
Gestión de identificaciones	0	1	0	0
Latencia de confirmación de transacción	1	1	0.5	0.5
Promedio	0, 625	1	0.125	0.25

Teniendo claro que la tecnología Blockchain mejor valorada fue Hyperledger-Fabric, esta permitirá mantener una comunicación cifrada entre los nodos de la red; además, de que cada nodo de la red estará totalmente identificado; por lo tanto, solo podrán realizar transacciones aquellos nodos que se encuentren autorizados dentro de la red; así mismo, al estar éstos conectados se podrá descentralizar información relevante que requieran tener todos los nodos. Lo anterior, debido a su libro distribuido permite que cada nodo pueda tener una copia exacta de dicho libro haciendo que si algún nodo de la red es atacado u en dado caso deja de funcionar por razones técnicas la red puede seguir operando y cuando el nodo vuelva a estar en funcionamiento puede sincronizarse nuevamente con toda la información que circuló mientras estaba fuera de línea.

VI. CONCLUSIONES

En la época actual es necesario incorporar tecnologías que sean capaces de brindar a las personas y organizaciones una mayor seguridad frente a sus datos confidenciales; es por ello que incorporar tecnologías como Blockchain en frameworks de ciberseguridad para IIoT resulta ser una gran alternativa puesto que garantiza la integridad de la información que emiten los dispositivos; además, de que dependiendo a la participación y enfoque que se le dé a esta tecnología ayuda a mantener un comunicación entre todos los nodos de la red garantizando un consenso en entre los mismos.

Por otra parte, es importante resaltar que las Blockchain de tipo públicas pueden ser que eviten sobrecargar el dispositivo con el procesamiento puesto que todo éste lo realiza el minero, pero tienen una limitante frente a la protección y confidencialidad de las transacciones, debido a que ésta al ser pública permite que cualquier individuo con conocimiento de las claves públicas del participante puede llegar a visualizar dichas transacciones logrando realizar una supervisión de las mismas. Es por este motivo que para entornos corporativos que manejan datos sensibles no es recomendable utilizar Blockchain de tipo públicas.

Como se puede observar en la caracterización la tecnología Blockchain que obtuvo una mejor puntuación de acuerdo a las características dadas fue Hyperledger-Fabric, por lo que es importante resaltar determinadas características que lo diferencian, entre ellas: su nivel de madurez en temas referentes a seguridad y privacidad de las transacciones realizadas puesto que su enfoque es permitir implementar Blockchain direccionadas hacia un entorno organizacional.

Las ventajas de implementar tecnologías Blockchain ligado a la ciberseguridad es la garantía de que la información que transita por toda la red es totalmente verídica e integra; por consiguiente, los usuarios pueden tener total garantía de dicha información; además de que éste tipo de tecnologías permite en cierto modo automatizar determinadas tareas que pueden llegar a ser tediosas con el tiempo cuando se tienen demasiados nodos en determinada red y se requiere sincronizar todos al mismo tiempo. Ahora, como toda tecnología también tiene sus puntos a considerar, ya que una

de las principales limitaciones es el almacenamiento, dado que como se sabe cada nodo tiene una copia exacta de todo el libro distribuido que contiene todas las transacciones y la información contenida en éstas, lo cual puede llegar a ser un problema con el tiempo y más aún en el caso de IoT que es un punto súper importante a considerar, como se sabe este almacenamiento es limitado; por esa razón, se deben tomar medidas que ayuden a mitigar dicha problemática.

AGRADECIMIENTOS

Agradecimientos a la Universidad del Cauca en especial a su grupo de investigación GTI y al grupo de investigación I+D en Informática de la Facultad de Ingeniería de la Institución Universitaria Colegio Mayor del Cauca, por el apoyo brindado para el desarrollo del proyecto.

REFERENCIAS

[1] S. Silvestre y J. Salazar, *El mundo Internet of Things (IoT)*, 2019, p. 28.

[2] J. J. Minguez, *IDS colaborativo basado en Blockchain,* Sevilla, 2019.

[3] Palo alto networks, «iotbusinessnews,» 2020. [En línea].

[4] J. Creswell, Planning, conducting and evaluating quantitative and qualitative research - Investigación educativa. Planeación, conducción y evaluación en investigación cuantitativa y cualitativa, vol. 4 , Pearson, 2012.

[5] Kaspersky, «latam.kaspersky.com,» 11 12 2020. [En línea]. Available: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security.

[6] F. Balmaseda aranda, *Aseguramiento de dispositivos IoT con blockchain e infraestructura de clave publica,* Madrid, 2018.

[7] B. Academy, «Cuántos tipos de blockchain existen,» Bit2me Academy, [En línea]. Available: https://academy.bit2me.com/cuantos-tipos-de-blockchain-hay/. [Último acceso: 08 08 2021].

[8] P. M. Cuéllar, «Blockchain, Smart Agro y Logística,» inforges, 17 12 2021. [En línea]. Available: https://www.inforges.es/post/blockchain-smart-agro-y-logistica. [Último acceso: 30 12 2021].

[9] B. Navarro, *Blockchain y sus aplicaciones*, 2017.

[10] E. Santiago y J. Sánchez, *RIESGOS DE CIBERSEGURIDAD EN LAS EMPRESAS*, Madrid, 2017.

[11] A. Valencia y P. Portilla, *Internet Industrial de las Cosas (IIOT): Nueva Forma de Fabricación.*

[12] J. Garcia, *DESARROLLO DE UN SISTEMA DE TRAZABILIDAD EN ENTORNOS IOT MEDIANTE HYPERLEDGER,* 2018.

[13] L. Chao, *Intrusion detection system for the internet of things based on blockchain and multi-agent systems,* 2020.

[14] H. Tian, *Research on distributed blockchain-based privacy-preserving and data security framework in IoT,* 2020.

[15] E. Berrocal y J. Expósito, *EL PROCESO DE INVESTIGACIÓN EDUCATIVA II: INVESTIGACIÓN-ACCIÓN,* 2017.

[16] A. Ali h, O. Nagwa M. y I. Hosny M., «Secured Framework for IoT Using Blockchain,» de *Ninth International Conference on Intelligent Computing and Information Systems(ICICIS)*, 2019.

[17] O. Alkadi, *A Deep Blockchain Framework-enabled Collaborative Intrusion Detection for Protecting IoT and Cloud Networks,* 2020.

[18] H. H. Pajooh y M. A. Rashid, «A Security Framework for IoT Authentication and Authorization based on Blockchain Technology,» de *18th IEEE International Conference On Trust, Security And Privacy In Computing And*, 2019.

[19] S. S. Panda, U. Satapathy, B. K. Mohanta, D. Jena y D. Gountia, *A Blockchain Based Decentralized Authentication,* 2019.

[20] U. Satapathy, B. K. Mohanta, S. S. Panda, S. Sobhanayak y D. Jena, *A Secure Framework for Communication in Internet of Things Application using Hyperledger based Blockchain,* 2019.

[21] G. Raja, A. Ganapathisubramaniyan, G. Anand y Gowshika, *Intrusion Detector for Blockchain based IoT Networks,* 2018.

[22] S. Rathore, B. W. Kwon y J. H. Park, *BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network,* 2019.

[23] M. A. Cheema, H. K. Qureshi, C. Chrysostomou y M. Lestas, «Utilizing Blockchain for Distributed Machine Learning based Intrusion Detection in Internet of Things,» de *16th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, 2020.

[24] B. Bhushan, C. Sahoo1, P. Sinha y A. Khamparia, *Unification of Blockchain and Internet of Things (BIoT): requirements, working model, challenges and future directions,* 2020.

[25] N. Shi, L. Tan, C. Yang, C. He, J. Xu, Y. Lu y H. Xu, *BacS: A blockchain-based access control scheme in distributed,* 2020.

[26] Pavithran, *Towards building a blockchain framework for IoT,* 2020.

Yeison Isaac Lucio LLante, Estudiante de décimo semestre de Ingeniería en Informática de la Institución Universitaria Colegio Mayor del Cauca, Colombia. Investigador en el área de Ciberseguridad e integrante del Semillero Beta Bit.

Katerine Márceles Villalba, Ingeniero de Sistemas de la Fundación Universitaria San Martín – sede Caribe, Colombia, Magister en Seguridad Informática de la Universidad Internacional de la Rioja, España. Investigador en el área de Ciberseguridad, Coordinador del Semillero Beta Bit de la Institución Universitaria Colegio Mayor del Cauca. Co-autor de varios libros y ponente en conferencias tanto a nivel nacional e internacional.

Siler Amador Donado, Ingeniero de Sistemas de la Universidad del Norte, Colombia, Magister en Seguridad Informática de la Universidad Internacional de la Rioja, España. Investigador en el área de Ciberseguridad, Coordinador del Semillero Security, Encryption & Cybersecurity de la Universidad del Cauca, Colombia. Co-autor de varios libros y ponente en conferencias tanto a nivel nacional e internacional.