

artículo original

Una Propuesta de Integración de Blockchain con Internet de las Cosas

A Proposal for the Integration of Blockchain with the Internet of Things

Mg. Jorge Eterovic ⁽¹⁾, Esp. Marcelo Cipriano ⁽²⁾, Lic. Edith Garcia ⁽³⁾, Lic. Luis Torres ⁽⁴⁾

⁽¹⁾ Departamento de Ingeniería e Investigaciones Tecnológicas. UNLaM
jorge.eterovic@gmail.com

⁽²⁾ Instituto de Investigación en Ciencia y Tecnología. Dirección de Investigación Vicerrectorado de Investigación y Desarrollo. USAL.
cipriano1.618@gmail.com

⁽³⁾ Instituto de Investigación en Ciencia y Tecnología. Dirección de Investigación Vicerrectorado de Investigación y Desarrollo. USAL.
edithxgarcia@gmail.com

⁽⁴⁾ Instituto de Investigación en Ciencia y Tecnología. Dirección de Investigación Vicerrectorado de Investigación y Desarrollo. USAL.
torreslu@ar.ibm.com

Resumen:

Internet de las cosas (IoT) ha extendido la conectividad de las computadoras a la mayoría de los dispositivos de nuestro entorno. IoT tiene el potencial de conectar millones de objetos simultáneamente intercambiando datos. Aunque los beneficios de IoT son ilimitados, existen muchos desafíos que enfrenta la adopción de esta

tecnología en el mundo real debido a su modelo cliente-servidor centralizado. Uno de los aspectos no resueltos es el problema de la seguridad. El modelo cliente-servidor requiere que todos los dispositivos estén conectados y autenticados a través de un servidor, lo que crea un único punto de falla.

Blockchain es una de las tecnologías más innovadoras de nuestro tiempo y su uso viene ganando interés desde su aparición gracias a su capacidad para asegurar la integridad de las transacciones y la autenticidad entre cualquier entidad conectada a Internet, de manera descentralizada, lo que significa que no hay un servidor maestro que albergue toda la cadena de transacciones. En su lugar, todos los nodos participantes tienen una copia de la cadena.

En este trabajo se hace una propuesta de integración de la tecnología Blockchain con IoT, destacando los beneficios y desafíos de dicha integración. También se presentan las futuras líneas de investigación de la integración de Blockchain con IoT. Se concluye que la combinación de Blockchain e IoT puede proporcionar un entorno más seguro que permita desarrollar nuevos modelos de negocios y aplicaciones distribuidas.

Abstract:

Internet of things (IoT) has extended the connectivity of computers to most of the devices in our environment. IoT has the potential to connect millions of objects simultaneously exchanging data. Although the benefits of IoT are unlimited, there are many challenges facing the adoption of this technology in the real world due to its centralized client-server model. One of the unresolved aspects is the security problem. The client-server model requires that all devices be connected and authenticated through a server, which creates a single point of failure.

Blockchain is one of the most innovative technologies of our time and its use has been gaining interest since its inception thanks to its ability to ensure the integrity of transactions and the authenticity between any entity connected to the Internet, in a decentralized manner, which means that no There is a master server that hosts the entire transaction chain. Instead, all participating nodes have a copy of the chain.

In this work a proposal is made for the integration of Blockchain technology with IoT, highlighting the benefits and challenges of such integration. Future research lines of the integration of Blockchain with IoT are also presented. It is concluded that the combination of Blockchain and IoT can provide a safer environment that allows developing new business models and distributed applications.

Palabras Clave: *Blockchain. Internet de la Cosas. Seguridad en Internet de las Cosas. Integración Blockchain con IoT.*

Key Words: *Blockchain. Internet of things. IoT security. Blockchain-IoT integration.*

I. INTRODUCCIÓN

Internet de las cosas (IoT) tiene la capacidad de conectar y comunicar millones de dispositivos simultáneamente. Esto está cambiando la forma en que las personas interactúan con la tecnología utilizando sensores y objetos interconectados para recopilar información de nuestro entorno, lo que permitirá mejorar nuestra calidad de vida [1].

El concepto de IoT no es nuevo. En 1999, Kevin Ashton fundador del Auto-ID Center en el MIT, dijo: "Internet de las cosas tiene el potencial de cambiar el mundo, tal como lo hizo Internet. Quizás aún más" [2]. Más tarde, en 2005, la UIT (Unión Internacional de Telecomunicaciones) definió oficialmente a IoT como "una infraestructura global para la sociedad de la información, que permite servicios avanzados mediante la interconexión de elementos (físicos y virtuales) interoperables, basados en las tecnologías de información y comunicación (TICs) existentes y en desarrollo" [3]

Los sistemas actuales de IoT se basan en el modelo cliente-servidor centralizado, que requiere que todos los dispositivos estén conectados y autenticados a través de un servidor. Como este modelo tiene un punto de falla fácilmente identificable, llevar el sistema IoT a una tecnología descentralizada puede ser una buena decisión. Una de las tecnologías descentralizadas existentes es Blockchain, que fue desarrollada por Stuart Haber y W. Scott Stornetta en 1991 [4].

Una cadena de bloques es una base de datos de registros distribuida que contiene todas las transacciones que se han ejecutado y compartido entre las partes participantes de la red. Esta base de datos distribuida se denomina libro

mayor distribuido. Cada transacción se almacena en el libro mayor distribuido y debe verificarse con el consentimiento de la mayoría de los participantes en la red. Todas las transacciones que se han realizado están contenidas en la cadena de bloques.

La integración de Blockchain con IoT podría tener muchos beneficios, además de eliminar el único punto de falla asociado con la arquitectura centralizada de IoT. El modelo descentralizado de Blockchain tiene la capacidad de gestionar el procesamiento de millones de transacciones entre los distintos dispositivos, lo que reducirá significativamente los costos asociados con la instalación y el mantenimiento de grandes centros de datos y distribuirá las necesidades de procesamiento y almacenamiento entre los millones de dispositivos que forman las redes de IoT. [5]. Además, la integración de Blockchain con IoT permitirá la mensajería entre pares, la distribución de archivos y la coordinación autónoma entre dispositivos IoT sin necesidad del modelo centralizado cliente-servidor [6].

En este trabajo se presenta una descripción general de la integración de Blockchain con la tecnología IoT, lo que implica un análisis de los beneficios resultantes del proceso de integración y los desafíos de implementación que se pueden encontrar. El objetivo final es proporcionar una descripción detallada de los beneficios y los desafíos que resultan de combinar Blockchain con IoT para plantear que la integración de Blockchain e IoT podría proporcionar una mejora a la seguridad aportando la integridad de las transacciones y la autenticidad entre cualquier entidad conectada a Internet.

ARQUITECTURA CENTRALIZADA DE IOT

Básicamente, IoT es la conexión y comunicación de diferentes dispositivos a través de Internet. Estos dispositivos están interconectados a través de los nodos de la red, ya sean servidores o computadoras, que a su vez se conectan entre sí para compartir sus datos. Todos los dispositivos cuentan con sensores que recopilan datos que pueden transmitirse, almacenarse, analizarse y presentarse de manera útil [7].

Actualmente existen muchas arquitecturas para IoT propuestas por diferentes investigadores y organizaciones.

Según la UIT, la arquitectura IoT se compone de cuatro capas como se muestra en la Fig. 1:

- Capa de aplicación
- Capa de soporte de servicio
- Capa de red
- Capa del dispositivo

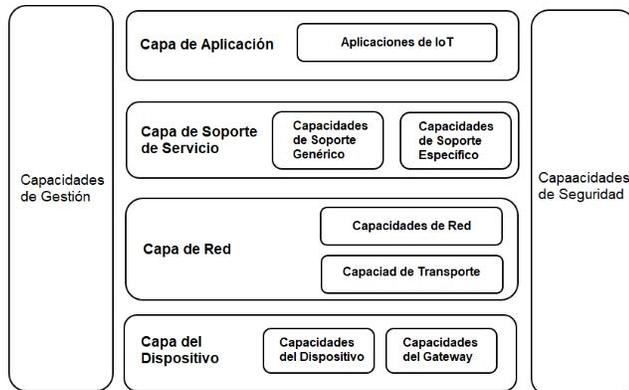


Fig. 1 Arquitectura IoT

La capa de aplicación abarca las aplicaciones de IoT. Hay muchas aplicaciones de IoT, como, por ejemplo: salud, ciudades inteligentes, automóviles conectados, gestión de energía inteligente, agricultura inteligente, administración de la cadena de suministros, monitoreo de la línea de producción, etc.

La capa de soporte de servicio contiene las capacidades comunes que pueden ser utilizadas por diferentes aplicaciones de IoT [8]. La capa de red incluye dispositivos como enrutadores, conmutadores, gateways

y firewalls que se utilizan para construir redes locales y de área amplia para proporcionar conectividad a Internet. Además, permite que los dispositivos se comuniquen entre sí y se comuniquen con plataformas de aplicaciones como computadoras, dispositivos de control remoto y teléfonos inteligentes.

La capa del dispositivo es similar a la capa física del modelo de interconexión de sistemas abiertos (OSI) de la arquitectura de red. Se compone de dispositivos físicos y controladores de objetos. Estos objetos representan cosas en el IoT que incluyen una amplia gama de dispositivos que envían y reciben datos. Por ejemplo, sensores que recopilan información sobre el entorno circundante [9].

La arquitectura actual de IoT se construye como un modelo centralizado que se conoce como modelo cliente-servidor. En este modelo, los dispositivos no pueden comunicarse entre sí, sino que se comunican con un gateway central. El modelo centralizado se ha utilizado para conectar una amplia gama de dispositivos informáticos durante muchos años y continuará admitiendo redes IoT a pequeña escala, sin embargo, no será capaz de satisfacer las necesidades crecientes de los futuros sistemas de IoT.

La cantidad de dispositivos IoT aumentará sustancialmente, estimándose que llegaría a 20 mil millones en el año 2020 [10], y en consecuencia aumentará la cantidad de comunicación que deberá gestionarse. El desafío de asegurar las comunicaciones seguirá siendo un aspecto a resolver ya que el modelo cliente-servidor tiene la vulnerabilidad de un servidor centralizado, que es el punto de falla que, de concretarse una amenaza, puede interrumpir las comunicaciones de toda la red [11].

Además, el modelo centralizado es vulnerable a la manipulación de datos. La recopilación de datos en tiempo real no garantiza que la información se use de manera adecuada. Por ejemplo, si las empresas proveedoras de energía descubrieran, a partir del análisis de los datos de los medidores inteligentes, que podrían ser objeto de una demanda judicial por parte de la Autoridad de Regulación de la Energía, podrían editar o eliminar estos datos [12]. Esta es una amenaza a la integridad.

Otra vulnerabilidad podría ser que se agreguen dispositivos falsos a una red IoT y generen información manipulada de manera tendenciosa. Esta es una amenaza a la autenticidad.

Una tecnología que podría mitigar estas amenazas a la seguridad de IoT es Blockchain.

TECNOLOGÍA BLOCKCHAIN

La tecnología Blockchain proporciona una forma eficiente de registrar transacciones o cualquier interacción digital de una manera que sea segura, transparente, altamente resistente a las interrupciones y auditable.

Blockchain se define como "una base de datos distribuida de registros, o libro mayor público de todas las transacciones o eventos digitales que se han ejecutado y compartido entre las partes participantes" [13]. Cada transacción en el libro mayor público se verifica por consenso de la mayoría de los participantes del sistema. Una vez ingresada, la información nunca se puede borrar. La cadena de bloques contiene un registro cierto y verificable de cada transacción realizada.

Una cadena de bloques consta de dos elementos principales, como se muestra en la Figura 2:

- Transacciones: son las acciones generadas por los participantes del sistema.
- Bloques: registra las transacciones, asegura que estén en la secuencia correcta y que no hayan sido manipuladas.

CARACTERÍSTICAS DE BLOCKCHAIN

Blockchain tiene algunas características que lo hacen muy atractivo para resolver muchos de los problemas de IoT. Estas características de Blockchain incluyen:

1. **Inmutabilidad:** construir libros de contabilidad inmutables es uno de los valores clave de Blockchain. Todas las bases de datos centralizadas se pueden dañar

y, por lo general, requieren confianza en un tercero para mantener la integridad de la información. Con Blockchain, una vez que haya acordado una transacción y se haya registrado, nunca podrá modificarse.

2. **Descentralización:** al no haber un control centralizado, se garantiza la escalabilidad y la solidez mediante el uso de recursos de todos los nodos participantes y se eliminan los flujos de tráfico del tipo "muchos a uno", lo que disminuye la latencia y resuelve el problema del punto único de falla que existe en el modelo centralizado.

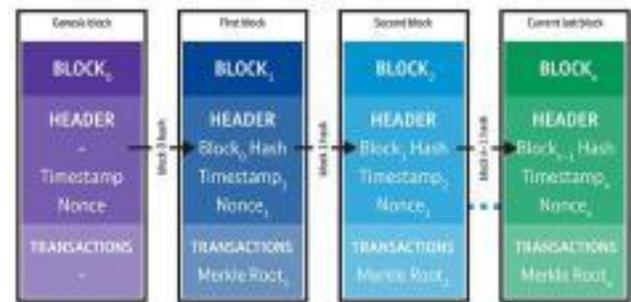


Fig. 2. Estructura de Blockchain

3. **Anonimato:** Blockchain proporciona una forma eficiente de ocultar la identidad de los usuarios manteniendo la privacidad.
4. **Más seguridad:** Blockchain proporciona más seguridad porque no hay un único punto de falla que, en caso de existir, al ser atacado, podría hacer colapsar a toda la red.
5. **Mayor capacidad:** uno de los aspectos más importantes de la tecnología Blockchain es que puede aumentar la capacidad de toda una red. Tener miles de computadoras trabajando en conjunto puede proveer

mayor potencia de cómputo que unos pocos servidores centralizados.

COMO TRABAJA BLOCKCHAIN

Aunque la tecnología Blockchain aún es nueva y está en fase de desarrollo y experimentación, se la percibe como una solución revolucionaria que aborda problemas tecnológicos modernos como la descentralización, la identidad, la confianza y la propiedad de los datos [14].

Blockchain es una base de datos que almacena todas las transacciones en bloques. Cuando se crea una nueva transacción, el remitente la transmite por el canal de comunicación “peer-to-peer” a todos los demás nodos de la red. La transacción aún es nueva y no está verificada. Cuando los nodos reciben la transacción, la validan y la mantienen en su libro mayor [15].

La validación de la transacción se realiza ejecutando chequeos predefinidos sobre la estructura y las acciones de la transacción. Un tipo de nodo especial llamado “minero” crea un nuevo bloque e incluye todas o algunas de las transacciones disponibles de un grupo de transacciones. Luego se hace la minería del bloque, que es un proceso para encontrar la prueba de trabajo (PoW) utilizando datos variables del encabezado del nuevo bloque. Encontrar la PoW es el cálculo continuo de un hash criptográfico que se ajuste al objetivo de dificultad predefinido.

La minería requiere mucha potencia de procesamiento y los mineros usan un hardware dedicado diseñado a tal fin. El minero que primero encuentra una solución para su bloque es el ganador. Su bloque candidato se convierte en el nuevo bloque de la cadena. Debido a que las

transacciones se agregan en el bloque de minería a medida que llegan, el último bloque en la cadena de bloques contiene las últimas transacciones.

Cuando se crea un nuevo bloque, se le agrega un sello de tiempo y se propaga a todos los nodos de la red. Cada nodo recibe el bloque, lo valida, con lo cual también valida las transacciones que contiene y agrega el bloque a su libro mayor. Cuando la mayoría de los nodos acepta el bloque, se convierte en una parte autorizada y no reversible de la cadena de bloques. Además de las transacciones, cada bloque almacena algunos metadatos y el valor del hash del bloque anterior. Entonces, cada bloque tiene un puntero a su bloque padre. Así es como se vinculan los bloques, creando una cadena de bloques llamada Blockchain.

El libro mayor distribuido está disponible para que todos en la red verifiquen los bloques y las transacciones que contiene. Sin embargo, los usuarios permanecen anónimos, solo se identifican por su clave pública. Además, las transacciones están cifradas. Las transacciones no válidas se rechazan y no se incluyen en los bloques. El intento malicioso de hacer un cambio en las transacciones requerirá repetir el cálculo de la PoW para el bloque que se quiere atacar y de todos los bloques posteriores. Estos cálculos no son factibles a menos que la mayoría de los nodos en la red sean maliciosos y colaboren en el ataque [16].

INTEGRACIÓN DE BLOCKCHAIN CON IOT

IoT es un sistema que proporciona beneficios ilimitados, pero existen muchas amenazas con la arquitectura actual de IoT, que es centralizada, de modo que todos los dispositivos se identifican, autentican y conectan a través

de los servidores centralizados. Este modelo se usó para conectar una amplia gama de dispositivos informáticos durante muchos años y continuará admitiendo redes IoT a pequeña escala, sin embargo, no será capaz de satisfacer las necesidades de crecimiento del sistema IoT en el futuro.

La Tabla 1 presenta una comparación de las principales características entre las tecnologías Blockchain e IoT. Hay ventajas en ambas tecnologías que pueden combinarse para obtener el mejor resultado. IoT tiene potencialidades ilimitadas y la adopción de un enfoque resolvería muchas amenazas, especialmente las de seguridad. La adopción de un modelo estandarizado de comunicación peer-to-peer para procesar los millones de transacciones entre dispositivos reduciría significativamente los costos asociados con la instalación y el mantenimiento de grandes centros de datos centralizados distribuyendo las necesidades de procesamiento y almacenamiento entre los millones de dispositivos que forman las redes IoT. Esto evitará que una falla en cualquier nodo provoque el colapso de toda la red.

Las capacidades descentralizadas, autónomas y de confianza de Blockchain lo convierten en la tecnología ideal para aportar soluciones a las amenazas de seguridad a IoT. No sorprende que las implementaciones de IoT empresariales hayan adoptado rápidamente la tecnología Blockchain. Sin embargo, al establecer las comunicaciones peer-to-peer se presenta un importante conjunto de desafíos, especialmente los referidos a la seguridad. La seguridad en IoT es mucho más que solo proteger datos confidenciales. Las soluciones Blockchain deberán mantener la privacidad y la seguridad en las redes de IoT y utilizar la validación y el consentimiento de los

participantes para las transacciones a fin de evitar la suplantación de identidad y el robo de información.

TABLA 2
COMPARACIÓN BLOCKCHAIN – IOT

Blockchain	IoT
Descentralizado	Centralizado
Alto consumo de recursos	Recursos restringidos
La minería de bloques consume mucho tiempo	Exige baja latencia
Escala mal a una red grande	Contiene una gran cantidad de dispositivos
Consumo mucho ancho de banda	Ancho de banda y recursos limitados
Tiene mejor seguridad	La seguridad es una de las amenazas de IoT

La tecnología Blockchain se considera clave para resolver los problemas de la integridad de las transacciones y de la autenticidad entre cualquier entidad conectada a Internet en IoT. Se puede utilizar para rastrear millones de dispositivos conectados, permitiendo el procesamiento de las transacciones y la coordinación entre dispositivos; Esto permite ahorros significativos para los fabricantes de la industria de IoT. Además, este enfoque descentralizado eliminaría puntos únicos de falla, creando un sistema más resistente para que los dispositivos funcionen. Los algoritmos criptográficos utilizados por Blockchain harían que los datos sean privados.

En una red IoT, la cadena de bloques puede mantener un registro inmutable de la historia de los dispositivos inteligentes. Esta característica permite el funcionamiento autónomo de dispositivos inteligentes sin la necesidad de una autoridad centralizada. Como resultado, Blockchain permitirá abrir una serie de escenarios de IoT que serían difíciles o incluso imposibles de implementar sin ella. Por ejemplo, al aprovechar la cadena de bloques, las

soluciones de IoT pueden permitir la mensajería segura y con confianza entre dispositivos en una red de IoT. En este modelo, la cadena de bloques tratará los intercambios de mensajes entre dispositivos como a las transacciones financieras en una red Bitcoin. Para permitir el intercambio de mensajes, los dispositivos podrían usar los contratos inteligentes que luego modelarán el acuerdo entre las dos partes.

Otra de las capacidades interesantes de Blockchain es la de mantener un libro de contabilidad confiable y descentralizado de todas las transacciones que ocurren en la red. Esta capacidad es esencial para permitir el cumplimiento y los requisitos reglamentarios de las aplicaciones industriales de IoT (IIoT) sin la necesidad de confiar en un modelo centralizado.

Muchas organizaciones grandes han comenzado a adoptar Blockchain con sistemas IoT para obtener todos los beneficios de Blockchain. Por ejemplo, IBM en asociación con Samsung ha desarrollado una plataforma ADEPT (Telemetría autónoma descentralizada punto a punto) que utiliza elementos del diseño subyacente de Bitcoin para construir una red distribuida de dispositivos, un IoT descentralizado. ADEPT utiliza tres protocolos BitTorrent (intercambio de archivos), Ethereum (Smart Contracts) y TeleHash (Peer to Peer Messaging) [11].

BENEFICIOS DE INTEGRAR BLOCKCHAIN

CON IOT

Hay muchos beneficios al integrar Blockchain con IoT. Estos beneficios se pueden resumir de la siguiente manera:

1.Privacidad: todos los participantes tienen la capacidad de ver todas las transacciones y todos los bloques, ya que cada participante tiene su propio libro mayor. El contenido de la transacción está protegido por la clave privada del participante [19], por lo que, si bien todos pueden ver las transacciones, no pueden leerlas porque los datos están protegidos. El IoT es un sistema dinámico en el que todos los dispositivos conectados pueden compartir información, pero al mismo tiempo deben proteger la privacidad de los usuarios.

2.Descentralización: la mayoría de los participantes deben verificar las transacciones para aprobarlas y agregarlas al libro mayor distribuido. No existe una autoridad única que pueda aprobar las transacciones o establecer reglas específicas para que las transacciones sean aceptadas. Por lo tanto, hay una gran cantidad de confianza incluida, ya que la mayoría de los participantes en la red tienen que llegar a un acuerdo para validar las transacciones. Por ello, Blockchain proporcionará una plataforma segura para dispositivos IoT. Además, elimina los flujos de tráfico centralizados y el punto único de falla de la arquitectura de IoT actual, que es centralizada.

3.Resiliencia: cada nodo tiene su propia copia del libro mayor que contiene todas las transacciones que se han realizado en la red, por lo que, la cadena de bloques puede resistir un ataque. Si un nodo estuviera comprometido, la cadena de bloques sería mantenida por cualquier otro nodo de la red. Tener una copia de datos en cada nodo en IoT mejorará los requerimientos de disponibilidad de información. Sin embargo, puede presentar nuevos problemas de procesamiento y almacenamiento por su baja disponibilidad de recursos.

4.Seguridad: Blockchain tiene la capacidad de proporcionar una red segura sobre partes no confiables, tal como lo necesita IoT con dispositivos numerosos y heterogéneos. Con Blockchain, todos los nodos de la red IoT, o la mayoría, deben ser maliciosos para que un ataque prospere.

5.Velocidad: una transacción de Blockchain se distribuye a través de la red en minutos y se procesará en cualquier momento durante todo el día.

6.Ahorro de costos: las soluciones de IoT actuales son costosas debido a la moderna infraestructura y el costo de mantenimiento asociado con la arquitectura centralizada, las granjas de servidores cada vez más grandes y los equipos de redes. La cantidad de comunicaciones que deberán gestionarse cuando haya millones de dispositivos IoT interconectados aumentará considerablemente los costos.

7.Inmutabilidad: tener un libro mayor inmutable es una de las principales ventajas de la tecnología Blockchain. Cualquier cambio en el libro mayor distribuido debe ser verificado por la mayoría de los nodos de la red. Por lo tanto, las transacciones no pueden ser alteradas o eliminadas fácilmente. Tener un libro de contabilidad inmutable para los datos de IoT aumentará la seguridad y la privacidad, que son los principales desafíos de la tecnología IoT.

8.Anonimato: para procesar la transacción, tanto el comprador como el vendedor usan números de dirección anónimos y únicos que mantienen privada su identidad. Esta característica ha sido criticada ya que aumenta el uso de criptomonedas en el mercado ilegal. Sin embargo,

podría verse como una ventaja si se utiliza para otros fines, como, por ejemplo, en los sistemas de voto electrónico.

DESAFÍOS DE INTEGRAR BLOCKCHAIN CON IOT

No hay duda de que la integración de Blockchain con IoT tendría muchas ventajas. Sin embargo, la tecnología Blockchain no es un modelo perfecto, ya que tiene sus defectos y desafíos. Estos desafíos se pueden resumir de la siguiente manera:

1.Escalabilidad: los problemas de escalabilidad en la cadena de bloques pueden conducir a la centralización, lo que arroja una sombra de duda sobre el futuro del Blockchain. La cadena de bloques escala mal a medida que aumenta el número de nodos en la red. Este problema es grave ya que se espera que las redes IoT cada vez contendrán más cantidad de nodos.

2.Poder de procesamiento y tiempo: este punto se refiere al poder de procesamiento y el tiempo necesario para lograr el cifrado de todos los objetos incluidos en un sistema Blockchain. Los sistemas IoT tienen diferentes tipos de dispositivos que tienen capacidades informáticas muy diferentes, y no todos podrán ejecutar los mismos algoritmos de cifrado a la velocidad requerida.

3.Almacenamiento: uno de los principales beneficios de Blockchain es que elimina la necesidad de un servidor central para almacenar las transacciones y los ID de los dispositivos. Entonces, el libro mayor debe almacenarse en los propios nodos. El libro mayor distribuido aumentará de tamaño a medida que pase el tiempo y con un número creciente de nodos en la red. Esto es un desafío,

ya que como se dijo anteriormente, los dispositivos IoT tienen bajos recursos computacionales y muy baja capacidad de almacenamiento.

4.Falta de personal capacitado: la tecnología Blockchain aún es nueva. Por lo tanto, pocas personas tienen grandes conocimientos y habilidades sobre la cadena de bloques. Entre los profesionales de la informática existe una falta de comprensión sobre el funcionamiento de la tecnología Blockchain, por lo que adoptar la cadena de bloques con IoT será muy difícil sin los conocimientos necesarios sobre Blockchain.

5.Aspectos legales y cumplimiento: Blockchain es una nueva tecnología que tendrá la capacidad de conectar a diferentes personas de diferentes países sin tener que seguir ningún código legal o de cumplimiento, lo cual es un problema grave tanto para los fabricantes como para los proveedores de servicios. Este desafío será la principal barrera para la adopción de Blockchain en muchas empresas y aplicaciones.

6.Nombramiento y descubrimiento: la tecnología Blockchain no se ha diseñado para IoT, lo que significa que los nodos no estaban destinados a encontrarse en la red. Un ejemplo es la aplicación de Bitcoin en la que las direcciones IP de algunos "remitentes" están integradas en el cliente de Bitcoin y son utilizadas por los nodos para construir la topología de la red. Este enfoque no funcionará para IoT ya que algunos dispositivos IoT se encuentran en movimiento todo el tiempo, lo que hará cambiará la topología continuamente.

FUTURAS LÍNEAS DE INVESTIGACIÓN

Blockchain ha cambiado el concepto de autoridades centralizadas. La integración de Blockchain con IoT será el punto de partida para desarrollar nuevos modelos de negocios y aplicaciones distribuidas. En esta sección se discuten las posibles futuras líneas de investigación sobre la integración de Blockchain con IoT. Estas tienen que ver con los Contratos Inteligentes, las Leyes y Regulaciones, la Seguridad y la nueva tecnología de contabilidad distribuida de código abierto: IOTA. Se pueden resumir de la siguiente manera:

CONTRATOS INTELIGENTES

Los contratos inteligentes son scripts almacenados en la cadena de bloques. Son tan poderosos debido a su flexibilidad, ya que pueden cifrar y almacenar datos de forma segura, restringir el acceso a los datos solo a las partes autorizadas y luego ser programados para utilizar los datos dentro de un flujo de trabajo lógico autoejecutable de las operaciones entre las partes. Los contratos inteligentes traducen el proceso comercial en un proceso informático, mejorando en gran medida la eficiencia operativa.

El uso de contratos inteligentes dentro de los sistemas IoT proporcionará una forma eficiente de mejorar la seguridad y la integridad de los datos de IoT. Las futuras líneas de investigación deberían responder las siguientes preguntas con respecto a la realización de contratos inteligentes en los sistemas IoT:

1:¿Son los contratos inteligentes capaces de ejecutar todas las funciones de los eventos que están en millones de dispositivos IoT?

2:¿Cómo responderá el contrato inteligente a las condiciones ambientales cambiantes del IoT?, ya que es un sistema dinámico.

3:¿Cuál es la plataforma adecuada para implementar contratos inteligentes dentro de los sistemas IoT?

LEYES Y REGULACIONES

Las leyes son los procedimientos creados por las autoridades y las agencias gubernamentales para definir formas legales de trabajar con un producto o tecnología dentro de un determinado país o región. Como se dijo anteriormente, el Blockchain es una nueva tecnología que no tiene ningún código legal o de cumplimiento a seguir. Las futuras líneas de investigación deberían responder la siguiente pregunta con respecto a los asuntos legales y de cumplimiento de Blockchain:

1:¿Cuáles son las leyes y regulaciones que garantizan las mejores prácticas del uso Blockchain en IoT a nivel mundial?

SEGURIDAD

Para todas las nuevas tecnologías, la seguridad sigue siendo el tema más desafiante que llama la atención de los investigadores y las organizaciones. La integración de Blockchain con IoT puede mejorar la seguridad, ya que utiliza el consentimiento de la mayoría de los participantes para validar las transacciones para evitar la suplantación de identidad y el robo de información. Sin embargo, los dispositivos IoT tienen bajos recursos de procesamiento y poco espacio de almacenamiento, por lo que no pueden procesar algoritmos criptográficos. Las futuras líneas de

investigación deberían responder las siguientes preguntas con respecto a la seguridad:

1:¿Cuál es la plataforma óptima para que IoT se integre con Blockchain?

2:¿Cómo superar las bajas capacidades de los dispositivos IoT para proporcionar un sistema IoT seguro?

IOTA

IOTA es una nueva generación de libro mayor público y distribuido que utiliza un concepto llamado "Tangle". El Tangle es una nueva estructura de datos que se basa en un Grafo Acíclico Dirigido (Directed Acyclic Graph - DAG). IOTA proporciona una transacción eficiente, segura, liviana, en tiempo real y sin cobro de comisiones. Tiene una arquitectura descentralizada de código abierto, diseñada específicamente para IoT.

Sin embargo, todavía está en desarrollo. Las futuras líneas de investigación deberían responder las siguientes preguntas con respecto a IOTA:

1:¿Cuál es la tecnología de descentralización adecuada para IoT? Blockchain o IOTA?

2:¿Cuáles son los principales desafíos para implementar IOTA?

CONCLUSIONES

La tecnología IoT se ha extendido a la industria y a todos los hogares. Tiene la capacidad de conectar objetos cotidianos a Internet. A través de sensores baratos, se puede recopilar mucha información del entorno que resulta en una mejora de nuestra calidad de vida. Sin

embargo, la arquitectura actual de IoT que se basa en el modelo cliente-servidor centralizado tiene muchos problemas que deben resolverse, especialmente la escalabilidad y la seguridad. Una de las opciones para abordar los problemas de IoT es usar la tecnología Blockchain. Esta tecnología proporciona una red de comunicación distribuida peer-to-peer donde los nodos no confiables pueden interactuar entre sí sin un intermediario confiable, de manera verificable. En este trabajo, se hace una descripción general de la integración de Blockchain con IoT, destacando los beneficios y desafíos a resolver. La discusión también se centró en futuras líneas de investigación. Finalmente, podemos concluir que la integración de Blockchain con IoT puede traer muchas soluciones que mejorarían algunos de los problemas de IoT, pero al mismo tiempo, se presentan nuevos desafíos que deberán abordarse. Es evidente que se necesita seguir investigando para lograr la integración de las tecnologías Blockchain con IoT para resolver algunos de los principales desafíos, como, por ejemplo: la seguridad y la privacidad.

AGRADECIMIENTOS

Este trabajo de investigación se desarrolló en el marco del Proyecto de Investigación “Análisis de la seguridad de los datos en Internet de las Cosas usando tecnología Blockchain”, que fue financiado por la Dirección de Investigación, dependiente del Vicerrectorado de Investigación y Desarrollo (VRID) de la Universidad del Salvador.

REFERENCIAS

[2] H. F. Atlam, A. Alenezi, R. J. Walters, and G. B. Wills, “An Overview of Risk Estimation Techniques in Risk-based Access Control for the Internet of Things,” in

Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security (IoTBDS 2017), 2017, pp. 254–260.

[3] K. Ashton, “That ‘Internet of Things’ Thing,” *RFiD J.*, p. 4986, 2009.

[4] ITU, “Overview of the Internet of things,” *Ser. Y Glob. Inf. infrastructure, internet Protoc. Asp. next-generation networks - Fram. Funct. Archit. Model.*, p. 22, 2012.

[5] Stuart Haber y W. Scott Stornetta; “How to Time-Stamp a Digital Document”; *Journal of Cryptology*, Vol. 3, No. 2, pp. 99-111; 1991.

[6] A. Banafa, “IoT and Blockchain Convergence: Benefits and Challenges,” *IEEE IoT Newsletter*, 2017. [Online].

Available: <http://iot.ieee.org/newsletter/january-2017/iot-and-blockchain-convergence-benefits-and-challenges.html>.

[6] E. Karafiloski, “Blockchain Solutions for Big Data Challenges A Literature Review,” in *IEEE EUROCON 2017 -17th International Conference on Smart Technologies*, 2017, no. July, pp. 6–8.

[7] W. Stallings, “The Internet of Things: Network and Security Architecture,” *Internet Protoc. J.*, vol. 18, no. 4, pp. 2–24, 2015.

[8] A. Torkaman and M. A. Seyyedi, “Analyzing IoT Reference Architecture Models,” *Int. J. Comput. Sci. Softw. Eng. ISSN*, vol. 5, no. 8, pp. 2409–4285, 2016.

[9] Cisco, “The Internet of Things Reference Model,” *White Pap.*, pp. 1–12, 2014.

[10] Nir Kshetri, “Can blockchain Strengthen the Internet of Things?” *IEEE Computer Society*, no. August, pp. 68–72, 2017.

[11] IBM, “ADEPT: An IoT Practitioner Perspective,” 2015.

[12] M. Conoscenti, D. Torino, A. Vetr, D. Torino, and J. C. De Martin, “Peer to Peer for Privacy and Decentralization in the Internet of Things,” in *2017 IEEE/ACM 39th IEEE International Conference on*

Software Engineering Companion Peer, 2017, pp. 288–290.

[13] A. Stanciu, “Blockchain based distributed control system for Edge Computing,” in 21st International Conference on Control Systems and Computer Science Blockchain, 2017, pp. 667–671.

[14] J. H. Ziegeldorf, F. Grossmann, M. Henze, N. Inden, and K. Wehrle, “CoinParty: Secure Multi-Party Mixing of

Bitcoins,” in Proceedings of the 5th ACM Conference on Data and Application Security and Privacy - CODASPY '15, 2015, no. August, pp. 75–86.

[15] M. Conoscenti, A. Vetro, and J. C. De Martin, “Blockchain for the Internet of Things: A systematic literature review,” 2016 IEEE/ACS 13th Int. Conf. Comput. Syst. Appl., pp. 1–6, 2016.

[16] A. M. Antonopoulos, Mastering Bitcoin: Unlocking Digital Cryptocurrencies. , M 1st ed. Sebastopol, CA, USA: O’Reilly Media, Inc., 2014.

Recibido: 2019-12-03

Aprobado: 2019-12-19

Hipervínculo Permanente: <https://reddi.unlam.edu.ar>

Datos de edición: Vol. 4 - Nro. 2 -Art. 1

Fecha de edición: Formato: 2020-01-31

