UNIVERSIDAD DE ESPECIALIDADES ESPÍRITU SANTO

Facultad de Ingeniería

Escuela de Sistemas

Análisis comparativo de un sistema de auditoría tradicional y un sistema de auditoría Blockchain e IPFS

Trabajo de Titulación que se presenta como requisito para el título de Ingeniero en Sistemas

Autor: Victor Joel Cuadros Choez

Tutor: Lohana Lema

Samborondón, 16 de junio del 2020

UEES
UNIVERSIDAD ESPIRITU SANTO

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del estudiante Victor Joel Cuadros Choez que cursa estudios en el programa de TERCER nivel: Ingeniería en Sistemas dictado en la Facultad de Sistemas, Telecomunicaciones y Electrónica de la UEES, en modalidad presencial.

CERTIFICO

Que he revisado el Trabajo de Titulación denominado: "Análisis comparativo de un sistema de auditoría tradicional y un sistema de auditoría Blockchain e IPFS", presentado por el estudiante Victor Joel Cuadros Choez, como requisito previo para optar por el Grado Académico de Ingeniero en Sistemas CERTIFICO que el Trabajo de Titulación ha sido analizado y reúne todos los requisitos para ser presentado y sometido a los procesos de revisión estipulados por la Facultad.

Atte.

Lohana Lema
0924554942

Análisis comparativo de un sistema de auditoría tradicional y un sistema de auditoría Blockchain e IPFS

Análisis comparativo de un sistema de auditoría tradicional y un sistema de auditoría Blockchain e IPFS

Victor Joel CUADROS CHOEZ

Resumen

El propósito del artículo es comparar la eficiencia, velocidad, seguridad, escalabilidad y performance de un sistema de auditoria tradicional y un sistema de auditoría Blockchain e IPFS (Interplanetary File System o Sistema de archivos interplanetarios) de almacenamiento de información cliente servidor, conocer problemas de sistemas de Auditorias actuales y exponer los beneficios de la implementación de un sistema de auditoría Blockchain e IPFS. El problema que se plantea es: ¿Qué tan alto es el nivel de seguridad y adaptabilidad que otorga este sistema de Blockchain para ser fiable en la auditoria de una empresa frente a un sistema tradicional? La metodología del estudio fue realizada con un enfoque cuantitativo que compara la Eficiencia, Velocidad, Seguridad, Escalabilidad, Performance de una arquitectura centralizada y una arquitectura descentralizada en un ambiente con una misma infraestructura. Se logró obtener información de la eficiencia, performance y escalabilidad del comportamiento que un sistema blockchain y el tradicional-relacional (SQL Server) que demostró en varios escenarios de cargas de archivos. Los resultados indican ventajas frente a un sistema tradicional. Conclusiones y recomendaciones: las ventajas de aplicar el sistema Blockchain es la simplificación del proceso de transmisión de datos lo que otorga mayor velocidad de trabajo, elimina intermediario, crea una atmosfera de transparencia.

Palabras clave: | Blockchain, IPFS, auditoria, big data, base de datos.

Abstract

The purpose of the article is to compare the efficiency, speed, security, scalability and performance of a traditional auditing system and a Blockchain and IPFS (Interplanetary File System) audit system for storing client client information, learning about current Audit systems and expose the benefits of implementing a Blockchain and IPFS audit system. The problem that arises is: How high is the level of security and adaptability that this Blockchain system provides to be reliable in the audit of a company compared to a traditional system? The study methodology was carried out with a quantitative approach that compares the Efficiency, Speed, Security, Scalability, Performance of a centralized architecture and a decentralized architecture in an environment with the same infrastructure. It was possible to obtain information on the efficiency, performance and scalability of the behavior that a blockchain and traditional-relational system (SQL Server) demonstrated in various file upload scenarios. The results indicate advantages over a traditional system. Conclusions and recommendations: the advantages of applying the Blockchain system is the simplification of the data transmission process, which gives greater speed of work, eliminates intermediary, creates an atmosphere of transparency.

Key words | Blockchain, IPFS, audit, big data, database.

INTRODUCCIÓN

Los sistemas computacionales comunes y en especial los sistemas bancarios, por su alta transaccionalidad, tienen la necesidad de tener un registro auditable e íntegro, para que su nivel de confiabilidad sea alto. Año a año gran parte de estos sistemas han sido vulnerados, repercutiendo en su confiabilidad. Un ejemplo de esto según Wilson Steven (2017) es el *Jackpotting*, un famoso software para hackear cajeros automáticos.

Continuamente a lo largo del tiempo, los sistemas se han enfocado en la encriptación de la información obteniendo como resultado el primer sistema de transferencia de criptomonedas conocido como bitcoin. La primera publicación científica de un sistema blockchain según Stornetta & Haber (1991), tiene como idea central tener un rastreo digital de archivos de audio, video, imagen o texto ordenado cronológicamente, permitiendo conocer con precisión su fecha de elaboración. En este sentido, según López (2018), el sistema blockchain no es una base de datos, aunque varios autores la definen como tal, como es el caso de Ocampo (2017), debido que su propósito principal no es albergar datos sino registrar transacciones, permitiendo una mejor trazabilidad en forma de big data, como lo menciona Dolader (2017).

Por otro lado, aunque esta tecnología fue utilizada originalmente para registrar el flujo de transacciones del bitcoin de acuerdo a Nakamoto (2008), con el pasar de los años se le ha evidenciado gran capacidad para ser aplicada en diversas industrias por las ventajas de las facultades que brinda, por ejemplo la creación de la criptomoneda Ethereum y sus programas computacionales Buterin (2015), otro ejemplo es la creación de *Storej*, siendo un prototipo de almacenamiento de archivos en blockchain Wilkinson (2014). Adicionalmente, brinda una base de datos distribuida e inalterable, basada en una serie progresiva de bloques. Aunque el sistema blockchain sea abierto permanece en un estado anónimo, para la seguridad de los usuarios, que se identifican con claves públicas o seudónimos según Nakamoto (2008). En la actualidad, se han ingresado más de 700 criptomonedas de forma global, de las cuales las más importantes son: Bitcoin, Ethereum, Bitcoin Cash, Ripple, Litecoin

Debido al gran número de funcionalidades que ya han sido demostradas en previas investigaciones como la de Valencia (2018), la cual menciona que la Banca es la industria en donde mayor impacto tiene la blockchain seguida de la industria de salud y alimentos. En la industria de la Salud, en Estonia su aplicación con el software Guardtime con mayor seguridad de información inclusive y actualización de fichas médicas o de PokitdoK o Healtnautica. También, en Estados Unidos, siendo el primer software que utiliza, procesa, confirma tratamientos y el segundo software conectado directamente pacientes y médicos, representan el inicio de la transformación en la salud. En industrias como la moda este sistema permite el rastreo en las materias primas y los procesos de fabricación mostrando la sostenibilidad y el cumplimiento de un artículo a sus consumidores.

Otro sector en crecimiento que menciona es el de energía; por ejemplo, *Grid Singularity* en países en desarrollo, o Powerpeers, en los Países Bajos por la empresa Vattenfall. Ambos en el área de la "generación distribuida", o el proyecto New 4.0 en Alemania que busca ser el primer mercado inteligente. Otro ejemplo en el área eléctrica es RWE en Europa, con el plan *Slock.it* que tramita la carga de los carros eléctricos a través de contratos inteligentes con Ethereum. La aplicación del sistema sigue en crecimiento, como ejemplo de aquello se puede observar su aplicación en Las Naciones Unidas (2018) donde están explorando cómo se puede utilizar Blockchain interna y externamente para abordar cuestiones humanitarias actuales, como el tráfico de niños, según Mahrinah von Schlegel, directora ejecutiva de la organización sin fines de lucro Embassy 2.0. la ONU utiliza actualmente Blockchain en 16 agencias, incluido el Programa Mundial de Alimentos (para ayudar a los refugiados a comprar alimentos) y la Oficina de Coordinación de Asuntos Humanitarios (para mejorar el financiamiento de los donantes, asegurar y monitorear las cadenas de suministro y datos protección) .

Según Muñoz, Boza, & Pablos (2018) afirma que "una de las características principales de blockchain como se ha mencionado con anterioridad es la seguridad". Puesto que contrario a un sistema tradicional o centralizado, donde se aloja todo en un servidor o grupo de servidores, esta tecnología permite crear bases de datos descentralizadas, compartidas y replicadas, las cuales solo son admisibles por usuarios autorizados. De esta manera, Palomo-Zurdo (2018), lo cataloga como el internet del valor o el internet de la confianza, debido al alto nivel de seguridad e inmutabilidad que posee.

En otro sentido, para facilitar la seguridad, y que los nodos del sistema blockchain permanezcan sin alteración, según Nakamoto (2008) se utiliza una recompensa económica en bitcoin, cuya finalidad radica en motivar a más personas a permanecer activos en los nodos de este sistema. De esta manera, si un atacante con ganas de robar bitcoin, fuera capaz de reunir más potencia CPU o GPU que la de todos los nodos del sistema, el beneficio seria nulo o quedaría en pérdida, porque bitcoin perdería valor y reunir esa potencia requiere más dinero que el hurtado. En el año 2008, con el

nacimiento de bitcoin y la creciente popularidad del mismo, se dio a conocer cómo funciona el blockchain y todos sus componentes. Actualmente existen dos tipos de blockchain populares en el mundo: públicos como (Bitcoin, Ethereum) y privados como (Blockchain de banca, transporte como Maersk).

A nivel de seguridad e innovación del blockchain, la iniciativa del creador de este sistema y los novedosos modelos de negocio que vendrán gracias al blockchain ha ocasionado que las personas piensen que el método centralizado ha fallado de forma personal como global. Es por esto que Andreessen (2014) fundador de Netscape, asegura que el blockchain es la invención más importante desde el internet, la cual puede tener diferentes aplicaciones como: bolsa de valores, registros médicos, notarias públicas, asientos contables inmutables, entre otras, como en el caso de esta investigación, un sistema de auditorías, y demás industrias donde ya se ha mencionado su aplicación según Nakamoto (2008).

En consecuencia, debido a los pocos trabajos sobre el tema, el presente trabajo tiene como objetivo demostrar la eficiencia, velocidad, seguridad, escalabilidad y performance de un sistema *blockchain* público usando *nodejs,* que es un entorno de tiempo de ejecución de JavaScript, sobre un sistema tradicional con una base de datos centralizada e IPFS, por sus beneficios descritos por Rusnak (2015) y Barrios (2014), son sus beneficios de almacenar archivos de forma descentralizada, confirmando así que mantener el registro de todas las transacciones da como resultado una auditoria confiable. Como primer objetivo especifico se busca describir los problemas de sistemas de Auditorias actuales. De segundo objetivo específico, exponer los beneficios de la implementación de un sistema de auditoría Blockchain e IPFS. Y como tercer objetivo específico, comparar un sistema tradicional de auditoria vs el sistema *blockchain.*

MARCO TEÓRICO

HISTORIA

El Blockchain fue creado y usado por primera vez en el año 2009, para poder dar vida a bitcoin de acuerdo a Nakamoto (2008). Desde ese entonces se buscaron inversionistas para iniciar la criptomoneda hasta su leve incremento de valor en el año 2012 y despliegue de popularidad a partir del 2013. Según la figura 1, donde también se observa un incremento y tope del bitcoin en 2017 diciembre a enero 2018, debido que China según Kaiser, Jurado, & Ledger (2018) aceptó como criptomoneda en 2013, es decir casi todas sus transacciones son realizadas en este país por sus distintas medidas regulatorias y la desmonetización de las monedas en los demás países. Por ejemplo, India y Venezuela sufren de una inflación insostenible lo cual ocasiona que de preferencia estos países vayan por una moneda virtual mucho más fuerte a su moneda. Según Agurto (2017), los principales factores por los cuales el bitcoin subió de precios son tres: La desmonetización global, la subida de bitcoin en China y la incertidumbre de la administración de Trump. Esta última según los análisis si Trump era elegido el bitcoin iba a subir de valor, lo cual si sucedió.

Figura 1.- Transacciones diarias de bitcoin desde 2009 - 2018
Fuente: (BLOCKCHAIN LUXEMBOURG S.A., 2018)

ESTRUCTURA DE UN BLOCKCHAIN

Respecto a su estructura, todo Blockchain se compone de partes clave para su funcionamiento, siendo el primero y más importante de ellos el bloque génesis Champagne (2014). Según Nakamoto (2008), "un Blockchain básico contiene algunos componentes claves para su funcionamiento" como son:

Bloque Genesis

Es el primer bloque de toda la cadena del blockchain, contiene su propio desglose, por el cual empieza:

Estructura	Bloque
Timestamp	20190101120000
Index	0
Data	N transacciones
Prev Block Hash	0000f23asaefd314
Nonce	1234

Index	Número del blockchain
TimeStamp	Fecha y hora en que se creó el bloque
Data	Contenido del bloque
PrevblockHash	Hash del bloque anterior
Difficulty	Número de zeros que debe tener el algoritmo hash
Total BTC	Valor de recompensa
MerKle Root	Árbol de decisiones
Size	Tamaño del bitcoin

Figura 2.- Descripción de un bloque
Fuente: Elaboración propia

Según Champagne (2014) "para entender un bloque génesis debemos imaginar un libro de contabilidad, en el cual, todos los miembros de la red blockchain comparten su libro mayor público, la cadena de bloques". Imagine un libro de contabilidad gigante con páginas que enumeran una serie de transacciones. Una nueva página que contiene las últimas transacciones del blockchain enviadas por pagadores de todo el mundo se agrega aproximadamente cada 10 minutos. Este libro gigante está constantemente disponible en Internet para quien ejecute el software Bitcoin.

Tener en cuenta que los programas llamados Bitcoin wallets (monederos) pueden ejecutarse en smartphones u ordenadores personales los mismos que permiten al usuario realizar pagos a través de la red Bitcoin. En el contexto de Bitcoin, las páginas que forman el libro mayor se llaman bloques porque representan "bloques" de datos. La cadena de bloques, compuesta por muchos bloques individuales, crece constantemente en longitud. Según Nakamoto (2008) la recompensa por cerrar un bloque en sus inicios constataba de 50 bitcoins de comisiones por transacción. Esta recompensa se va modificando cada cuatro años, a la mitad sin afectar las comisiones. En la actualidad, el incentivo por acertar con un hash para cierre de bloque válido es 12.5 bitcoins de comisiones. De esta manera, una vez se ha cerrado un grupo de transacciones o un bloque y se ha adquirido la prueba correspondiente por medio del cálculo de hashes, el minero deberá añadir en ese bloque una transacción con el valor de la recompensa a su cuenta de Bitcoin.

Según Martínez-Cabrera (2014) "merkle root" (Árbol Merkle) es estructura de datos estratificada y organizada, parecido a un árbol de dictamen estadístico combinado por varios hashes. Se utiliza por razones de confirmación, seguridad y de manera de entendimiento de datos; en la parte alta del merkle root está situado el "Hash Raíz" que es el que ayuda como forma de confirmación de datos. Un caso de ejemplo del hash raíz en una operación peer to peer. Al momento de extraer los diferentes bloques informativos que contiene el archivo o mensaje de la transacción, se crearía el hash raíz de una forma confidencial y confiable. De esta manera interactuar con los otros nodos. Asimismo, se obtendrá el hash raíz de cualquier cuenta con el que se entable comunicación de forma directa y se verificará con el de confiabilidad alta o creado recientemente, de esta manera, las cuentas con malas intenciones o con el contenido falso serán denegadas en el método post de toda la red y sus nodos que tienen el hash correcto; además, sirve como manera de entendimiento de información en la medida en que la plenitud de cada rama del árbol puede ser verificada de manera inmediata sin requerir de la totalidad del árbol, por medio del hash compuesto de datos y la comparación con la raíz.

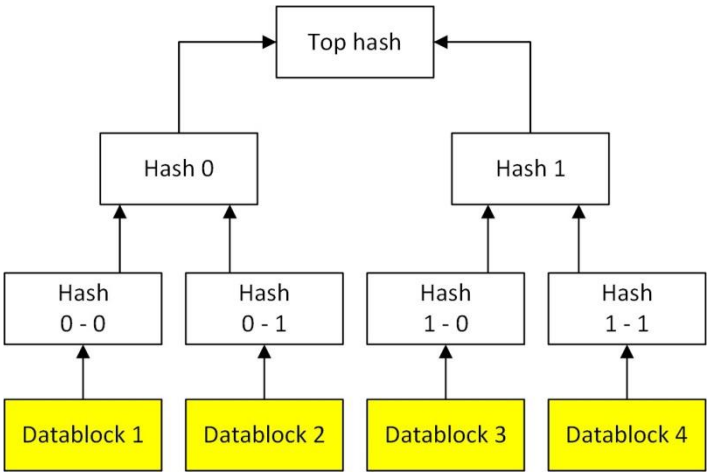

Figura 3.- Árbol de ejemplo de merkle root
Fuente: Elaboración propia

- **Nonce**

El nonce es un número al azar por el cual efectúa la regla de la dificultad. Dicha dificultad depende de que tan rápido se está resolviendo el algoritmo por lo cual se va ajustando de manera automática. La regla es encontrar un número que permita tener cierta cantidad de ceros precedentes en el hash. Actualmente, aquella persona que encuentre el nonce para encontrar el hash con los ocho ceros podrá obtener la recompensa.

Block 0 o Genesis

Hash:	00000000000081cd02ab7e569e8bcd9317e2fe99f2de44d49ab2b8851ba4a308
Bloque siguiente:	000000000000aa7802ab7e569e8bcd9317e2fe99f2de44d49ab2b885bcdaa113
Tiempo:	03/01/2009 18:15
Dificultad:	1(Bits:1d00fff f
Transacción:	1
Total BTC:	50
Tamaño:	285 bytes
Merkle root:	4a5e1e4baab89f3a32518a88c31bc87f6184f76673e2cc77ab2127b7afdeda33b
Nonce:	2083236893
Raw Block	

Transacciones

Transaccion	Fee	Tamaño(kB)	De (monto)	To (monto)
4a5e1e4baab…	0	0,204	Generacion:50 + total comisión	1A1zP1eP5QGefi2DMPTffL5SLmv7DivfNa: 50

Figura 4: Bloque Genesis
Fuente: Elaboración Propia

Incentivo

Según (Nakamoto, 2008), el incentivo en simple concepto consiste en mantener a los usuarios minando para mantener nodos activos y se cierren los bloques, el incentivo puede ayudar a que los nodos permanezcan honestos.

Algoritmo hash

De acuerdo a (Gutiérrez, 2013) el objetivo principal es crear una cadena que solo puede obtenida nuevamente, solo y solo si, tiene los mismos datos, es decir el valor alfanumérico obtenido es un resumen de la información el cual, si se altera un valor, no se genera otra salida diferente de información. El hash como tal es inhackeable y no se puede repetir, de tal forma que la seguridad del blockchain es alta.

Prueba de trabajo

El concepto prueba de trabajo fue inventado por Adam Back en 1997, según Back (2002) es un algoritmo hash se ha utilizado como una técnica de medida de contador de denegación de servicio en varios sistemas, creado específicamente para evitar spams de emails, el algoritmo funciona con un valor hash criptográfico, como SHA1, SHA256 o SHA3 los cuales son muy seguros e inclusive usados en bancos.

Tipos de blockchain

Según Preukschat (2017) existen tres tipos de blockchain:

- Públicas
    - Los ejemplos más claros son Bitcoin y Ethereum, por públicas se definen porque pueden ser accedidas desde cualquier lado del mundo, solo requieren una computadora e internet.
- Privadas
    - Los ejemplos de blockchain privada es, hyperledger, R3 y Ripple, por lo general son usados en instituciones financieras o empresas privadas.
- Hibridas
    - Podemos citar de ejemplo BigchainDB y Evernym, cada nodo es un invitado o un usuario privado pero toda transacción realizada existe de forma pública.

Mineros

De acuerdo a Dolader (2017) los mineros se deben ver como nodos de la red que pertenecen en el proceso de ingreso de información en la blockchain a cambio de un incentivo económico. La veracidad y legibilidad de la información ingresada es revisada por todos los participantes. Una vez el minero ganador cumple su tarea le es acreditado un incentivo que se acreditara en el próximo cierre del bloque.

Generaciones de blockchain

Actualmente existen 3 generaciones de blockchain, conformadas por la primera como la conocemos netamente transaccional, representada por el bitcoin, la segunda como Ethereum va más allá de las transaccionalidad y se complementa con los contratos inteligentes, asignando un set de reglas a cada transacción o contrato, por último, la tercera generación se ha dividido en algunos focos, por ejemplo hay casos en que se enfocan en almacenamiento de archivos, en otros en escalar la solución a otro nivel y solucionar la debilidad del bitcoin en la actualidad.

Blockchain y su crecimiento

Actualmente, podemos ver un crecimiento constante en proyectos y temas de búsqueda en blockchain a nivel web. Según la figura 5 el crecimiento va de forma ascendente y constante.

Figura 5: Crecimiento de uso de blockchain en proyectos
Fuente: Análisis de Deloitte de datos de GH Torrent y GitHub API, octubre 12,2017

Según la figura 6 se puede observar que existe un crecimiento a nivel organizacional sobre blockchain e interés en el tema en base al nivel de aceptación del mismo.

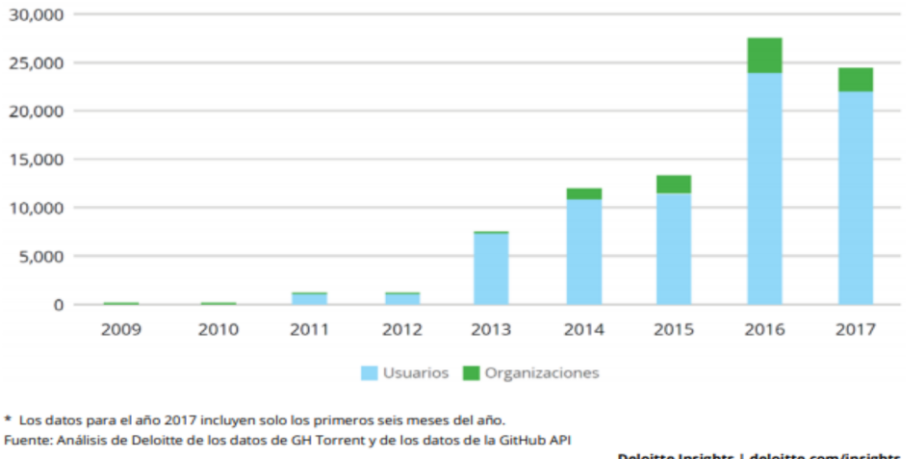

Figura 6: Crecimiento de uso de blockchain a nivel organizacional
Fuente: Análisis de Deloitte de datos de GH Torrent y de los datos de GitHub API

Entre las diferentes criptomonedas podemos encontrar desde las iniciales como lo es bitcoin, la primera criptomoneda, a las más actuales como Corda.

Cuando blockchain fue introducido al público, la idea de Nakamoto (2008) no ha cambiado en lo absoluto, un blockchain basado en una red de criptomoneda, los mismos que son unidos y encriptados en una cadena inhackeable. La única variante del sistema ha sido su valor de premio o ganancia por encontrar el algoritmo hash, disminuyendo su valor.

Ethereum y su creador Buterin (2015), decidió llevar más allá la tecnología blockchain e incluir contratos inteligentes, su fin era quitar la limitante de bitcoin a nivel transaccional a un nivel de contratos inteligentes, donde podemos asignar reglas para completar transacciones y brindar la seguridad y fiabilidad de un blockchain.

Corda es un opensource basado en Ethereum, cuya finalidad es ir a la tercera generación de blockchain y ser escalable, buscando las bondades del opensource donde toda persona pueda contribuir al fin.

Lenguajes de programación

Actualmente una solución de blockchain tiene diferentes aspectos y usos, para poder desarrollarlo una solución en blockchain se debe programar utilizar nodejs y programar en javascript, python y solidity, este último siendo un lenguaje nativo para Ethereum.

Los IDE más comunes son editores de texto como visual studio code, notepad++ y en su nivel más básico Notepad.

IPFS

Conocido por sus siglas en ingles Interplanetary file system (IPFS) según el Departamento de Electrónica, Universidad Técnica Federico Santa María, IPFS es un sistema de archivos distribuidos que busca conectar todos los computadores con el mismo sistema de archivos.

Un sistema IPFS tiene como finalidad:

Como un sistema de archivos global, usando IPFS.

- Como un archivo de actualización automática de versiones, publicaciones y respaldos, tipo GitHub.
- Como un sistema de file-sharing.
- Como un administrador de versiones de paquete para software.
- Como una plataforma conectada y encriptada de comunicación.
- Como un CDN con integridad comprobada para archivos grandes.
- Como un CDN encriptado
- Como una red permanente donde los links no mueren.

En resumen, como es bien sabido el blockchain básicamente es un backend descentralizado, IPFS en resumen es un front end descentralizado, tal como se aparece en la figura 7.

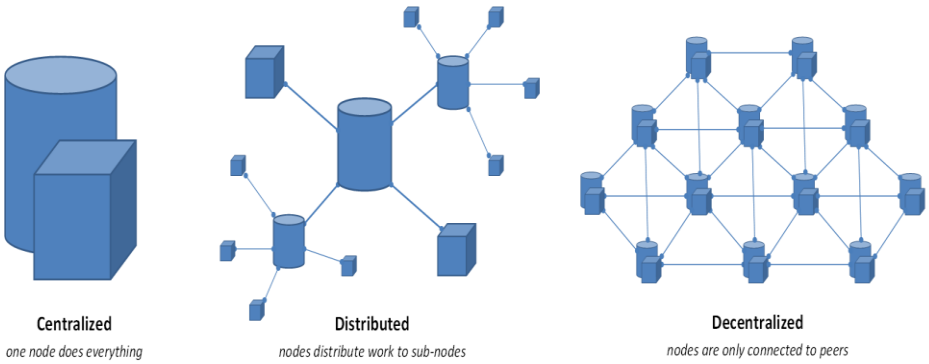

Figura 7: Crecimiento de uso de blockchain en proyectos
Fuente: Mesh World P2P Simulation Hypothesis, Febrero 02,2016

Sistemas de auditoria actuales

Un sistema de auditorías tiene varios objetivos como seguridad, control y trazabilidad. Actualmente todas las bases de datos se manejan de forma centralizada y algunas con réplicas de la contingencia de la base de datos principal donde los datos son sincronizados continuamente. Las bases de datos más usadas de acuerdo a Arsenault (2017) son:

- MySQL
- Oracle 12c.
- Microsoft SQL Server
- DB2
- PostgreSQL
- SAP HANA
- MongoDB
- MariaDB

Normalmente al elegir una base de datos las primeras preguntas que surgen son:

- ¿Qué cantidad de datos voy a transmitir?
- ¿A cuántos clientes quiero brindar el servicio de manera continua?
- ¿Qué requerimiento de tiempo de respuesta requiero brindar a mis clientes?
- ¿Voy a implementar trabajos en “batch” o masivos que tendrán acceso a los datos?
- ¿Cómo voy a escalar mi infraestructura según vaya incrementándose el número de transacciones?
- ¿Qué tipo de base de datos necesito?
- ¿Como voy a monitorear mis datos y tener el tiempo de caída más bajo?
- ¿Como se comporta con problemas de caída?

La recomendación general para mantener una base de datos segura, de acuerdo al sitio web Acens (2015) son:

- Identificar sensibilidad
- Evaluación de vulnerabilidades
- Auditar cambios
- Monitorizar toda actividad en la base de datos
- Control de acceso

Problema de los sistemas de auditorías actuales

En su mayoría, las bases de datos ofrecen encriptación y niveles de seguridad, pero a pesar

de estos esfuerzos, el administrador del sistema siempre tendrá la libertad de modificar esta información.

El mayor peligro en todo sistema es editar la información, lo cual es fácilmente realizado con una sentencia de update en los sistemas más sencillos sin encriptación. En el caso de ser los sistemas más seguros generan un log transaccional los cuales también pueden ser editados.

Adicional las vulnerabilidades más comunes de acuerdo a Acens (2015) son:

- Usuario o password débil
- Asignar a grupos incorrectos para accesos
- Deshabilitar características innecesarias
- Actualizar sistema de base de datos para cubrir bugs o puertas traseras

Solución usando blockchain

Aprovechando las bondades del blockchain a nivel transaccional y del IPFS a nivel de frontend, ambas teniendo como prioridad la descentralización de la información y seguridad, se podrá llegar a una solución escalable para temas de auditoria.

METODOLOGÍA

La presente investigación aplicará una metodología con enfoque cuantitativo, que compara Eficiencia, Velocidad, Seguridad, Escalabilidad, Performance o prueba de stress de una arquitectura centralizada y una arquitectura descentralizada tal como se muestra en la Figura 8 y Figura 9 respectivamente, en un ambiente con una misma infraestructura. La arquitectura está compuesta por una capa backend, middleware y web para consumo del middleware como servicio, en ambas arquitecturas.

Para medir la métrica de velocidad, se tomará tiempos de respuesta a nivel de backend y aplicación. Para medir la eficiencia y performance se realizará una prueba de estrés, subiendo el mismo archivo en 100 ocasiones. Otra medida que va vinculada a la velocidad es la seguridad, se medirán los tiempos de respuesta de la data encriptada y desencriptada para evidenciar como afecta al performance a una capa extra de seguridad. Una vez obtenida esta información la escalabilidad del equipo en su arquitectura se medirá y evidenciará los beneficios de cada uno de estos sistemas.

Con este contraste de resultados, se podrá evidenciar en donde cada una de estas arquitecturas destaca más y tener una idea de todos los casos de uso que podremos aplicar ambas arquitecturas.

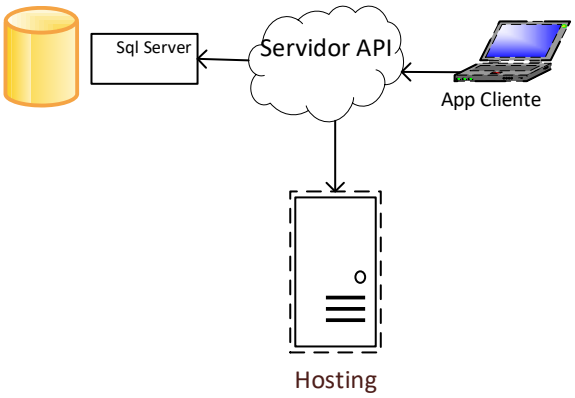

Figura 8: Arquitectura de sistema tradicional centralizado
Fuente: Elaboración propia

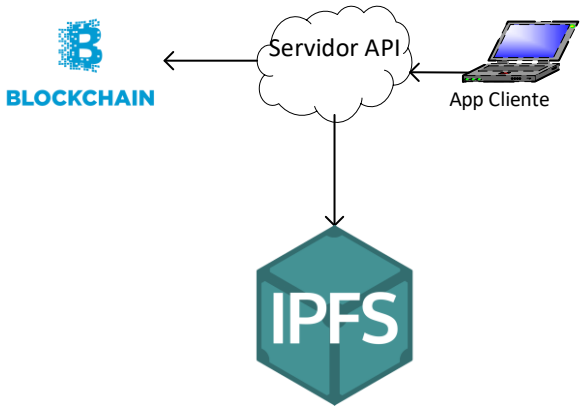

Figura 9: Arquitectura de sistema descentralizado Blockchain
Fuente: Elaboración propia

DESARROLLO

El método de comprobación fue comparando los dos sistemas, el tradicional centralizado y el descentralizado. Las características serían las siguientes:

Sistema tradicional centralizado características:

- Procesador: Intel Core i7-6700HQ 2.60Ghz 2.59Ghz
- Memoria ram: 16 GB
- Sistema operativo: Windows 10 enterprise
- Base de datos: SQL server 2016
- Lenguaje de programación: Visual studio .NET

Se creó una aplicación en .NET, ejecutada en el backend para ejecución de una operación en forma de cascada, la cual lee un archivo .csv y por cada registro insertará una fila en la base de datos y subirá un archivo al servidor con tamaño de 1 Mb

Sistema descentralizado:

- Procesador: Intel Core i7-6700HQ 2.60Ghz 2.59Ghz
- Memoria ram: 16 GB
- Sistema operativo: Windows 10 enterprise
- Base de datos: Blockchain
- Lenguaje de programación: .net node.js

Para recibir la información de la aplicación .NET, se creó un api con node.js, el cual recibe la siguiente información:

- AppId
- Usuario origen
- Usuario Destino
- Nombre del archivo
- Extensión del archivo
- Archivo a subir

Esta información es almacenada dentro del blockchain y el archivo en el ipfs. Se creó una aplicación en .NET la cual lee un archivo .csv y por cada fila enviará los registros necesarios en el api y subirá un archivo al ipfs. Las métricas a medir son las siguientes:

- Eficiencia
- Velocidad
- Seguridad
- Escalabilidad
- Performance o prueba de stress

En el caso de pruebas individuales se configuró la aplicación postman, la cual es una cliente para consumir apis y poder hacer pruebas. Adicional tambien se configuró el sistema ANTS para poder recopilar la informacion necesaria para obtener los resultados de forma correcta.

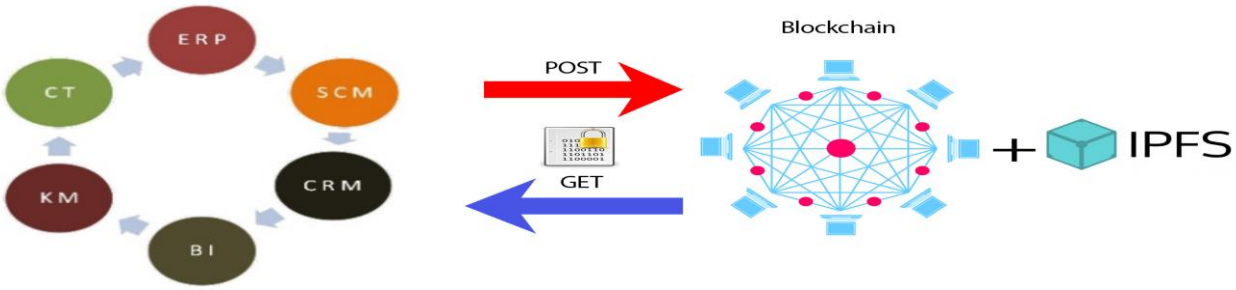

Figura 10: Diseño de consumo de API en blockchain.
Fuente: Elaboración propia

Eficiencia

Se puso a prueba la eficiencia midiendo las ventajas de ambas aplicaciones, con arquitectura centralizada y descentralizada.

1. En ambos sistemas se subieron 100 archivos de forma simultánea.
2. El sistema cliente en cada arquitectura se inicializará como un servicio, almacenando el archivo en un hosting y el ipfs respectivamente.
3. Los tiempos se almacenaron en un archivo texto.
4. Se realizaron varias pruebas y se midió un tiempo promedio.

Velocidad: En ambos sistemas se subió 1 archivo con la aplicación Postman como cliente como se observa en la Figura 11 y Figura 12.

1. Los tiempos se almacenaron en un archivo texto.
2. Se realizaron varias pruebas y se midió un tiempo promedio.

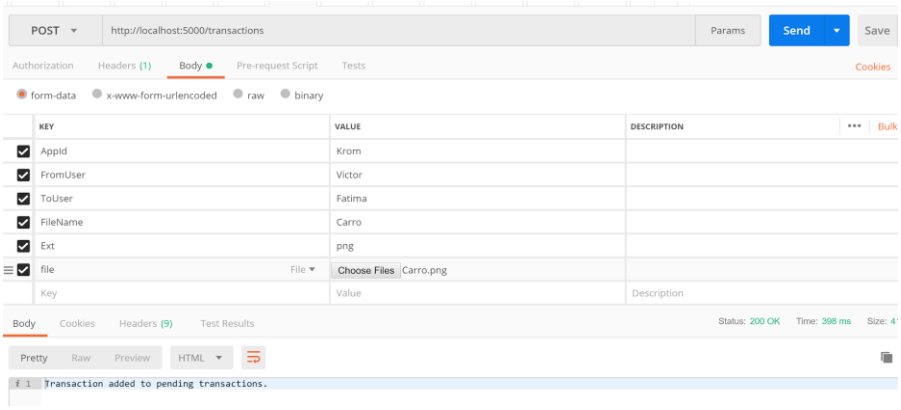

Figura 11: Ingreso de datos en Postman
Fuente: Elaboración propia

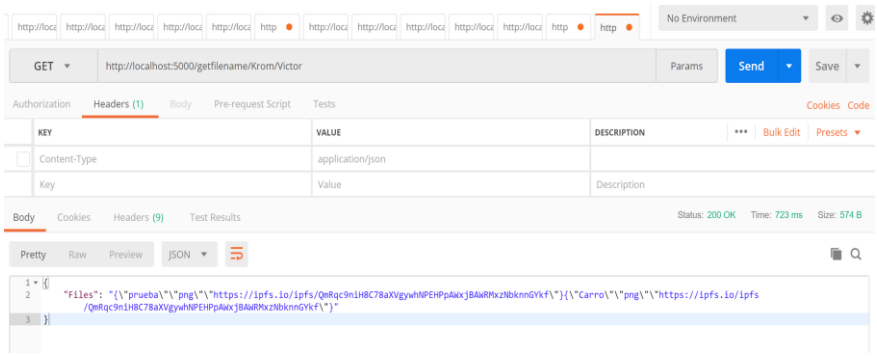

FIgura 12: Resultado de Api en sistema no centralizado en cliente Postman
Fuente: Elaboración propia

Seguridad:

1. En ambos sistemas se subieron 100 archivos de forma simultánea.
2. El sistema centralizado fue encriptado para simular el nivel de encriptamiento de blockchain, pero en lugar de hash se utilizó TDE.
3. Los tiempos se almacenaron en un archivo texto.
4. Se realizaron varias pruebas y se midió un tiempo promedio con los datos encriptados en el sistema centralizado.

Escalabilidad:

Para el sistema en blockchain se abrieron varios nodos para revisar como se divide la carga de

trabajo y comprobar su funcionalidad versus la de un sistema tradicional donde solo se puede escalar en el mismo equipo virtual limitándolo a las características del equipo físico. Adicional la escalabilidad se midió a nivel costo beneficio, en un sistema cloud como azure.

Performance:

El performance se medirá por medio del software ANTS mediante el cual se verificará la cantidad de recursos que utiliza cada aplicación mientras se realiza la prueba de eficiencia.

ANÁLISIS DE RESULTADOS

Eficiencia:

En la aplicación con IPFS se llevó la ventaja debido a que en IPFS si se sube el mismo archivo consecutivamente, no lo vuelve a subir, revisa si lo tiene en base y si ya lo tiene solo anexa el mismo Hash. En el caso del sistema tradicional, sube el archivo tantas veces sea sin verificación de que si existe o no. Se evidencia este modo de subir archivos a la nube en la tabla 1, al comparar los tiempos de subida, es más eficiente Blockchain con una ventaja de casi 350 veces más rápido.

Escenarios	100 mismo archivo	100 diferentes archivos
Blockchain + IPFS	00:00:01:030	00:00:24:92
Sistema tradicional	00:05:49:99	00:05:49:99
Sistema tradicional encriptado	00:06:11:68 - 00:06:30:98	00:06:11:68 - 00:06:30:98

Tabla 1: Resultados Eficiencia

Velocidad:

Los resultados en velocidad son evidentes a favor del sistema descentralizado, los cuales se pueden evidenciar en la Tabla 1 que está dividida en horas: minutos: segundos: milisegundos. Se obtuvieron resultados evidentes subiendo diferentes archivos, dando como resultado que el sistema blockchain es 11 veces más rápido que el sistema tradiciona

Seguridad:

La aplicación de auditoria tiene como vulnerabilidad principal en el sistema centralizado, se realizaron pruebas con un nivel de encriptación a nivel de base de datos para tener seguridad de data TDE, pero esto afectó la velocidad aumentando de un 5% a un 10% desencriptando la información teniendo como resultados variables.

Se define como vulnerabilidad si la persona encargada tiene el código fuente o conocimiento de base de datos para alterar la información del sistema de auditoria no obstante haber usado secuenciales como clave primaria. A diferencia del sistema tradicional el sistema de auditoria con Blockchain e IPFS, no tiene esos problemas porque para alterar un dato de la cadena se alteraría toda la cadena futura y el uso de secuenciales es reemplazado por el flujo de la cadena lo cual no ha sido posible alterarlo.

Escalabilidad:

La escalabilidad como costo beneficio, podemos concluir que es mucho más beneficioso comprar varios equipos con mayor GPU y poder transaccionar sin inconveniente en un sistema blockchain a diferencia de un equipo o servidor de alto valor donde utiliza CPU o varios equipos con alto CPU en un sistema con Blockchain no es beneficios a tener más GPU porque es más costoso. En la Tabla 2 podemos observar que con el mismo equipo utilizando CPU vs GPU tenemos una gran diferencia en tiempos.

Adicional a estos valores expuestos en la tabla dos no se cuentan con valor que si están presenten en Azure VM como energía eléctrica, internet disponibilidad.

Equipo	Nucleos	Hilos	Hilos Totales	Precio Mensual	Precio anual	Precio a 3 años
ASUS ZENBOOK UX501VW	4	8	32	$62,50	$750,00	$2.250,00
Azure VM serie B	2	24	48	$89,94	$1.079,28	$3.237,84
ASUS ZENBOOK UX501VW x3	12	8	96	$187,50	$2.250,00	$6.750,00
Azure VM serie B	4	24	96	$156,22	$1.874,64	$5.623,92

Tabla 2: Resultado de Tiempos

Performance:

Al utilizar la herramienta ANTS se puede concluir que a nivel de performance consumen la misma cantidad de recursos en un solo equipo, menos del 5% de CPU del equipo, al utilizar otro nodo en

El blockchain esta carga se divide a 2.5% por equipo, el problema principal del blockchain radica en que si la cadena es muy grande y hay pocos equipos el performance se deterioraría drásticamente.

CONCLUSIONES, LIMITACIONES Y TRABAJOS FUTUROS.

Una vez realizada la investigación se puede determinar dos puntos claves, las ventajas de usar un sistema blockchain debido a sus características de trabajo y las facilidad de aplicación y adaptación en los modelos de negocios y diversas industrias donde se puede aplicar esta tecnología. Entre las ventajas de aplicar el sistema Blockchain es la simplificación del proceso de transmisión de datos lo que otorga mayor velocidad de trabajo, elimina intermediario, crea una atmosfera de transparencia al dar una visión más clara de la procedencia de las transacciones, rastrear la información de forma más sencilla y procesar el historial de forma permanente, y al unir todas estas ventajas da mayor seguridad al salvaguardar los intercambios de datos y garantizar la seguridad de todos los involucrados descentralización de la información garantiza su inmutabilidad. De esta manera da la oportunidad a futuras aplicaciones y motivación a emprender en esta nueva tecnología paras obtener la mayor ventaja.

Las limitaciones de aplicación de la presente investigación están relacionadas a la cantidad de equipos disponibles con los cuales se pudieron realizar la conexión de nodos en el sistema con blockchain y las variaciones que podría afectar diferentes velocidad y corte de internet. Otra limitante es una comparativa a nivel de GPU vs CPU, debido a que no se contaba con los equipos requeridos para la prueba.

Es importante señalar que con los datos obtenidos en la presente investigación pueden ser considerados para trabajos futuros al realizar estudios en diferentes modelos de negocios e industrias superando las limitaciones presentadas estudiando cómo afecta eso a la velocidad del blockchain.

Bibliografía

Aguto, S. (2017, abril 11). *El valor del bitcoin se dispara a nivel mundial, ¿cuál es la causa?* Retrieved from genbeta: https://www.genbeta.com/a-fondo/el-valor-del-bitcoin-se-dispara-a-nivel-mundial-cual-es-la-causa

Arsenault, C. (2017, Abril 20). *The Pros and Cons of 8 Popular Databases*. Retrieved from keycdn: https://www.keycdn.com/blog/popular-databases

Back, A. (2002). *Hashcash - A Denial of Service Counter-Measure.*

Buterin, V. (2015). *Ethereum white paper.*

Carlos Dolader, J. B. (2017). *LA BLOCKCHAIN: FUNDAMENTOS, APLICACIONES Y RELACIÓN CON OTRAS TECNOLOGÍAS DISRUPTIVAS.*

Champagne, P. (2014). *ElLibro deSatoshi.*

Club Innovación. (2018). *Blockchain Público vs Privado*. Retrieved from Club Innovación: http://www.clubdeinnovacion.com/bloginn/blockchain-publico-privado

Grange, E. (2016, febrero 18). Retrieved from delphitools: https://www.delphitools.info/DWSH/

Gutierrez, P. (2013, enero 15). *¿Qué son y para qué sirven los hash?: funciones de resumen y firmas digitales*. Retrieved from genbeta: https://www.genbeta.com/desarrollo/que-son-y-para-que-sirven-los-hash-funciones-de-resumen-y-firmas-digitales

Jesus Leal Trujillo, S. F. (2017). *Evolution of blockchain technology Insights from the GitHub platform.* Deloitte Insights.

Jesus Leal Trujillo, S. F. (2017). *Evolution of blockchain technology Insights from the GitHub platform.*

Kaiser, B., Jurado, M., & Ledger, A. (2018). *The Looming Threat of China:An Analysis of Chinese Influence on Bitcoin.*

López, M. A. (2018). *Blockchain Cómo desarrollar confianza en entornos complejos para generar valor de impacto social. .*

Martínez-Cabrera, J. S. (2014). *Bitcoins. ¿Revolución o Historia?*

La historia del blockchain en 3 generaciones. (2018, 07 23). Retrieved from Espacio del Inversionista:https://espaciodelinversionista.wordpress.com/2018/07/23/la-historia-del-blockchain-en-3-generaciones/

Muñoz, A., Boza, M. H., & Pablos, J. I. (2018). *Introducción a los mecanismos de seguridad basados en tecnología blockchain.*

Nakamoto, S. (2008). *Bitcoin: un sistema de dinero en efectivo electrónico peer-to-peer1.*

OCampo Mayor, C. E. (2017). *Blockchain la nueva base de datos no sql en big data.* Bogota.
Palomo-Zurdo, R. (2018). *Blockchain: la desentralizacion del poder y su aplicacion en la defensa.*

Preukschat, A. (2017). *BLOCKCHAIN:LA REVOLUCIÓN INDUSTRIAL DE INTERNET.*

Stornetta, W. S., & Haber, S. (1991). *How to Time-Stamp a Digital Document.*

Valencia, F. C. (2018). *Tecnología Blockchain: elementos básicos, aplicaciones y marcos regulatorios.*

Wilkinson, S. (2014). *A Peer-to-Peer Cloud Storage Network.*

Hill, K. (2014). Bitcoin Battle: Warren Buffett vs. Marc Andreessen. Forbes.

BAUMGART y S. MIES. (2007). *A practicable approach towards secure key-based routing, en IN PARALLEL AND DISTRIBUTED SYSTEMS*

Nishara Nizamuddin (2018*). IPFS-Blockchain-based Authenticity of Online Publications*

Wilson Steven (2017). *Cashing in on ATM Malware: A Comprehensive Look at Various Attack Types*

Jeimy J. Cano (2004). *Inseguridad informática: Un concepto dual en seguridad informática*

AcensTechnologies (2010). *Bases de datos y sus vulnerabilidades más comunes*

Paul Rusnak (2015). *IPFS*

Matías Barrios (2014). *IPFS: Interplanetary File System*

Calculadora de precios. (n.d.). Obtenido de https://azure.microsoft.com/es-es/pricing/calculator/

Benet, Juan. (2014) *IPFS - Content Addressed, Versioned, P2P File System.*

K. Toyoda. (2017) *A Novel Blockchain-Based Product Ownership Management System (POMS) for Anti-Counterfeits in The Post Supply Chain*,