ESCUELA COLOMBIANA DE INGENIERÍA JULIO GARAVITO

TRABAJO DE GRADO

Blockchain aplicado en ambito no financiero

Autor:
Ing. Fabio Enrique QUINTERO DiazGranados

Supervisor:
Ing. Luis Daniel BENAVIDES Navarro

Trabajo de grado para optar por el título de Master en Gestión de Información

en

CTG-informática
Maestría en Gestión de Información

28 de septiembre de 2018

Declaración de Autoría

Yo, Ing. Fabio Enrique QUINTERO DiazGranados, declaro que este trabajo de grado titulado como, «Blockchain aplicado en ambito no financiero» y el trabajo por completo presentado es de mi autoria. Yo confirmo que:

- Declaro ser consciente que cualquier tipo de fraude en este Trabajo de Investigación es considerado como una falta al reglamento de la Escuela Colombiana de Ingeniería Julio Garavito.
- Firmar, entregar y presentar esta propuesta de Trabajo de Investigación implica expreso testimonio de que esta propuesta fue desarrollada de acuerdo con las normas establecidas por la Escuela Colombiana de Ingeniería Julio Garavito
- Me comprometo a seguir estrictamente las normas de derechos de autor.
- No haré publicaciones, informes, artículos o presentaciones en congresos, seminarios o conferencias sin la revisión o autorización expresa del Director, quien representará en este caso a la Escuela Colombiana de Ingeniería Julio Garavito.

Estudiante: _____

Fecha: _____

Director: _____

Fecha: _____

«Thanks to my solid academic training, today I can write hundreds of words on virtually any topic without possessing a shred of information, which is how I got a good job in journalism.»

Dave Barry

ESCUELA COLOMBIANA DE INGENIERÍA JULIO GARAVITO

Resumen

Ingeniería de Sistemas
Maestría en Gestión de Información

Master en Gestión de Información

Blockchain aplicado en ambito no financiero

por Ing. Fabio Enrique QUINTERO DiazGranados

This work is deep research about how Blockchain should help and improve daily process, those process related to transactions would be taken with enhanced security, anonymity and decentralized ...

Agradecimientos

Agradezco profundamente a mi esposa y mi hijo por ser diariamente mi fuerza y mi motivación para ser cada día mejor, también por permitirme tomar de nuestro tiempo familiar para poder lograr este documento.
A mis padres que me forjaron a ser quien soy, mi mamá en especial por su apoyo constante en cada locura que se me ocurre.
Al Ing. Luis Daniel BENAVIDES Navarro por la dedicación, paciencia y esfuerzo durante la consecución de este documento ...

Índice general

Índice de figuras

Índice de cuadros

Lista de abreviaturas

LAH	**L**ist **A**bbreviations **H**ere
WSF	**W**hat (it) **S**tands **F**or

Constantes Físicas

Speed of Light $c_0 = 2.997\,924\,58 \times 10^8\,\mathrm{m\,s^{-1}}$ (exact)

Lista de símbolos

a	distance	m
P	power	W ($\mathrm{J\,s^{-1}}$)
ω	angular frequency	rad

Dedicado a mi hijo Fabio Andrés

Capítulo 1

Descripción del proyecto

1.1. Resumen del proyecto

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aliquam ultricies lacinia euismod. Nam tempus risus in dolor rhoncus in interdum enim tincidunt. Donec vel nunc neque. In condimentum ullamcorper quam non consequat. Fusce sagittis tempor feugiat. Fusce magna erat, molestie eu convallis ut, tempus sed arcu. Quisque molestie, ante a tincidunt ullamcorper, sapien enim dignissim lacus, in semper nibh erat lobortis purus. Integer dapibus ligula ac risus convallis pellentesque.

1.2. Planteamiento del problema

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aliquam ultricies lacinia euismod. Nam tempus risus in dolor rhoncus in interdum enim tincidunt. Donec vel nunc neque. In condimentum ullamcorper quam non consequat. Fusce sagittis tempor feugiat. Fusce magna erat, molestie eu convallis ut, tempus sed arcu. Quisque molestie, ante a tincidunt ullamcorper, sapien enim dignissim lacus, in semper nibh erat lobortis purus. Integer dapibus ligula ac risus convallis pellentesque.

1.2.1. Planteamiento

Nunc posuere quam at lectus tristique eu ultrices augue venenatis. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Aliquam erat volutpat. Vivamus sodales tortor eget quam adipiscing in vulputate ante ullamcorper. Sed eros ante, lacinia et sollicitudin et, aliquam sit amet augue. In hac habitasse platea dictumst.

1.2.2. Formulación

Nunc posuere quam at lectus tristique eu ultrices augue venenatis. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Aliquam erat volutpat. Vivamus sodales tortor eget quam adipiscing in vulputate ante ullamcorper. Sed eros ante, lacinia et sollicitudin et, aliquam sit amet augue. In hac habitasse platea dictumst.

1.3. Estado del arte

Blockchain es una tecnología reciente y revolucionaria donde se establece una nueva arquitectura(Iansiti y Lakhani, 2017), esto es que, se basa en la confianza de los nodos de la red, plantea eliminar a los terceros o intermediarios que hacen las validaciones y generan la confianza necesaria entre los dos participantes de la transacción, por lo tanto existe una aprobación general en la red frente a una transacción que puede ser verificada en cualquier momento en el pasado o el presente (Crosby y col., 2016)
Blockchain se comporta como un libro de transacciones, basado en cifrado lo cual garantiza la transparencia y seguridad en cada transacción, sin ahondar técnicamente en su funcionamiento podemos indicar que cada transaccion es inalterable, aunque de fondo lo es, podría ser dectectado el fraude con facilidad y descartando la cadena en cuestión, por lo tanto en un símil un bloque, con un conjunto de transacciones, puede ser alterado pero del mismo modo podrá ser dectectado y descartado por los nodos honestos de la red (Nakamoto, 2009)
Y si bien durante este proceso hemos mencionado que es una conjunto de registros distribuido y que gracias al cifrado podemos garantizar la transparencia en las transacciones, también, se pueden anonimizar las transacciones ya que no es necesario saber quien la realiza sino solo su identificador público (clave pública) (Crosby y col., 2016), basado en la tecnologia de cifrado publico/privado garantizamos que los registros son irrefutables (*IC y Blockchain: retos y riesgos*) y que de por si garantiza la comunicación entre las partes (Iansiti y Lakhani, 2017)

1.3.1. Contratos inteligentes

Son basicamente un conjunto de reglas programadas que ejecutan los terminos de un contrato de forma automatica al cumplirse o no estas condiciones (Crosby y col., 2016) Basados en que Blockchain tiene control de algunas variables como tiempo (Kosba y col., 2016) y los participantes de una transacción es practicamente un trabajo adicional que se apalanquen los contratos a una tecnología implementada con Blockchain que permitirá verificar controlar y ejecutar con mayor facilidad.

1.3.2. Propiedades Inteligentes

“Es otro concepto relacionado al control de un activo/bien/propiedad mediante los contratos inteligentes "(Crosby y col., 2016)

1.3.3. Monedas colereadas

Si respresentamos los objetos existentes en una transacción con una etiqueta (colorear el objeto) para marcar a ese objeto como si fuera en realidad un representación del mundo real (activo/bien/propiedad), eje. unas acciones. De esta forma se puede almacenar los movimientos de estos en las transacciones pero idetificando claramente a cada una de estas etiquetas.
Se podría poner la propiedad de un auto o una casa en una transacción y moverla de un propietario a otro. (Crosby y col., 2016)

1.3.4. Aplicaciones

Valores privados

Las bolsas de valores listan acciones de la compañía en un mercado secundario para funcionar de forma segura con operaciones de liquidación y compensación de manera oportuna, ahora es posible para las empresas que emitan directamente las acciones a través de Blockchain. Estas acciones puede ser compradas y vendidas en un mercado que se encuentra en la cadena de bloques. (Crosby y col., 2016)

Notariado público

Gracias a las características de Blockchain las cuales garantizan que las transacciones son firmadas por el creador y receptor, que cada transaccción se registre con una marca de tiempo y se mantenga la transparencia e integridad son garantias que un documento tendrá un creador y que este documento fue creado en un momento de tiempo y que el registro de ese documento se mantendrá en el tiempo inmutable. (Zheng y col., 2016)
Podemos adicionar que esto elimina la necesidad de que un tercero valide alguna de las caracterisitcas previas sino que de la misma forma este documento estará distribuido a lo largo de la red lo cual generará que los costos del proceso disminuyan (Crosby y col., 2016)
Para el 2018 en Colombia el gobierno está apalancando en esta tecnología para su proyecto de restitución de tierras[1] a personas victimas del conflicto armado.

Propiedad intelectual

Si bien cualquier recurso digital se le puede aplicar el modelo de blockchain, a medio electronicos como películas, canciones y demás que involucren propiedad intelectual les impacta de buena forma está tecnología ya que con esta tecnología será garante de que no se puedan generar duplicaciones no autorizadas. (Huckle y col., 2016)
"Aquí es donde el blockchain puede jugar un papel. La tecnología puede ayudar a mantener una gran base de datos distribuida precisa de la propiedad de los derechos musicales información en un libro público. Adicionalmente a la información de propiedad de derechos, la división de regalías para cada trabajo, según lo determinado por Smart Contracts, podría ser agregado a la base de datos. Esta Los contratos inteligentes a su vez definirían las relaciones de relación entre diferentes partes interesadas y automatizar sus interacciones" (Crosby y col., 2016)

Intenet de las cosas

Internet de las cosas (IoT por sus siglas en ingles) es una tencnología emergente y que con seguridad no ha logrado su máximo de madurez, al igual que Blockchain, IoT tiene como finalidad integrar los elemento de nuestro diario vivir con nosotros de formas autonomas y transparentes.
En el comercio electrónico se esta proponiendo un nuevo modelo basado en Blockchain y contratos inteligentes de propiedades inteligentes, la idea es que las personas reciban transacciones al cumplirse una condición a partir de señales de sensores emitidas por

[1] **https://www.elespectador.com/economia/asi-se-utiliza-blockchain-para-garantizar-la-restitucion-de-tierras-articulo-809025**.

los objetos inteligentes. (Zheng y col., 2016)
Para añadir otro elemento Blockchain puede proveer una descentralizada red que habilita a los objetos inteligentes a interactuar con criptomonedas y garantizar que todas sus interacciones estan completamente validadas por la red(Crosby y col., 2016), de esta forma los usuarios podrán tener tranquilidad que ningun dispositivo podrá ser vulnerado o manipulado en beneficio o en contra de un usuario.
Un ejemplo con una tecnología emergente hace un par de años y que ahora parece consolidarse un poco es Uber, está podría implementar un modelo de IoT y Blockchain; para cuando un pasajero llega a su destino el cobro se implemente de inmediato mediante contratos inteligentes, pero de la misma forma cuando el conductor de Uber no garantiza el servicio el pasajero se puede ver beneficiado cobrando una multa por un mal servicio o daño en la reputación por alguna circustancia.(Huckle y col., 2016)

Cuidado de la salud

Uno de los campos de acción de Blockchain es permitir garantizar la identidad de los pacientes, un paciente debidamente carnetizado y enrolado permite que toda su información sea el unico que puede acceder a ella y permitir a quienes les da acceso para que sea consultada. (Angraal, Krumholz y Schulz, 2017) Pero sin lugar a dudas lo más beneficioso para un paciente es que puede aprovechar la ventaja de que su historia está distribuida y como se beneficia de esto, supongamos un paciente crónico alérgico a una gran cantidad de medicamentos y/o compuestos químicos tantos como para no poder mencionarlos todos o un paciente con una gran cantidad de cirugias a lo largo de su vida, como hacen ahora para poder cambiar de ubicación? pues deben llevar su historia médica en papeles, Blockchain llega al rescate todo estará disponible para ser consultado cualquier médico autorizado podrá revisarlo con los conceptos de sus colegas no solo lo que recuerda el paciente.
Esto nos lleva a otro uso y es que entre aplicaciones que usan la tecnología se podría compartir información de un paciente, podrían compartir autorizaciones, permisos y acuerdos firmados, esto sería de gran ayuda para reducir los tiempos de procesos entre organizaciones que prestan servicios de salud. (Angraal, Krumholz y Schulz, 2017)

1.3.5. Retos de blockchain

Regulación

El tema regulatorio es bastante discutible, la tecnología siempre avanza mucho mas rápido que los gobiernos, en especial latino americano, como es de esperarse Blockchain se está asentando y el gobierno aun no ve la necesidad de hacerlo, lo difícil de esta postura es que cuando se vea en la necesidad puede que sea muy restrictivo impactando de forma negativa e impidiendo todo su potencial(*IC y Blockchain: retos y riesgos*), permitiendo que solo algunos se benficien de este mismo como menciona (Arias, 2018) deberá ser equilibrado y regular lo suficiente para impedir que se use de forma fraudulenta y también proteger al más debil.

Escalabilidad

El constante crecimiento de la base de datos, con un tamaño 100,18 GB [2], todas las transacciones deben ser almacenadas para poder validar cada transacción, además que por definición el tiempo entre bloques de transacciones tiene un retraso de tiempo lo que lleva a que se procesen solo 7 transacciones por segundo lo que lleva a que en un mundo donde se implemente esta tencnología impediría que se use en tiempo real (Zheng y col., 2016)
Además si un usuario es nuevo en el ecosistema y pretende hacer una transacción debera primero sincornizar su base de datos descargando toda la cadena de bloques y validar las transacciones antes de poder realizar su transacción lo cual le tomará un tiempo en ejecutar (Crosby y col., 2016)

Resistencia al cambio

Como en todo proyecto de tecnología, por lo general innovadores, se debe hacer la gestión del cambio para no impedir que los actores generen resitencia y el proyecto fracase en una organización, en este caso puede que no sea una organización pero si el público en general puede ser renuente al uso, debido a que se pueden generar mitos sobre el uso de la tecnología como problemas de seguridad, ineficiencia, lentidtud, etc. En la actualidad los intermediarios (eje. Visa, masteercard, Uber)(Crosby y col., 2016) brindan la seguridad que ningun problema se pueda presentar (aun cuando se presentan) y son garantes de que las transacciones se cumplan con satisfacción de las partes.

Integración con el pasado

Uno de los grandes problemas que se pueden presentar en la aplicación de la tenoclogía es la historia existente, primero el problema que conlleva la migración de esta historia implicaría tiempo y costos altos(Crosby y col., 2016) y ademas ya que de alguna forma se debe integrar pero toda esta historia se registrarían como nuevas transacciones en la cadena y se generaría confusiones y si no se tiene cuidado el orden de documentos, por ejemplo podría alterarse cronologicamente si no se hace un uso adecuado, aunque este reto propiamente afecta a la organización que quiera aplicar está tecnología deberá tener en cuenta un proyecto alterno de gestión del conocimiento por ejemplo, para mitigar este riesgo.

Fraude

Debido a la naturaleza de Blockchain se pueden presentar intentos de fraude, pero como se indica en el artículo originar de Blockchain se espera que el esfuerzo tan alto de hacer fraude se vea mejor recompensado por el hecho de hacer el esfuerzo por mantener un cadena de bloques honesta(Nakamoto, 2009), pero en algún punto el camino tenderá a torcerse y deberá mantenerse controles y regulaciones para controlar estos intentos de una forma certera, encaminados con regulaciones de ley para que la comunidad se sienta protegida

[2] cifras 2016

Súper computadoras

La capacidad de computo es una de las piedras angulares de Blockchain y la prueba de trabajo es un control de varios elementos del protocolo Blockchain, por lo tanto si llegará a existir alguna super computadora que siempre estuviera en la capacidad de generar primero la prueba de esfuerzo implicaría que la dificultad (Nakamoto, 2009) deberá aunmentar hasta que los mineros puedan generarlo aleatoriamente, pero por obvias razones los demas mineros continuaran en desventaja ya que su capacidad de computo es menor.
Pero ahora si, como es de esperarse, la capacidad de computo de la comunidad minera comienza a mejorar la difcultad, como se mencionó antes, debe aumentar pero existe una limitante en esa dificultad y es que la cantidad de ceros no puede crecer infinitamente por que si no no quedará espacio para la información lo que obligaría al protocolo a migrar de algoritmo de seguridad con implicaciones e impactos para la red elevados(Crosby y col., 2016)

1.4. Objetivos del proyecto

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aliquam ultricies lacinia euismod. Nam tempus risus in dolor rhoncus in interdum enim tincidunt. Donec vel nunc neque. In condimentum ullamcorper quam non consequat. Fusce sagittis tempor feugiat. Fusce magna erat, molestie eu convallis ut, tempus sed arcu. Quisque molestie, ante a tincidunt ullamcorper, sapien enim dignissim lacus, in semper nibh erat lobortis purus. Integer dapibus ligula ac risus convallis pellentesque.

1.4.1. Objetivo general

Nunc posuere quam at lectus tristique eu ultrices augue venenatis. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Aliquam erat volutpat. Vivamus sodales tortor eget quam adipiscing in vulputate ante ullamcorper. Sed eros ante, lacinia et sollicitudin et, aliquam sit amet augue. In hac habitasse platea dictumst.

1.4.2. Objetivos específicos

- Nunc posuere quam at lectus tristique eu ultrices augue venenatis. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Aliquam erat volutpat. Vivamus sodales tortor eget quam adipiscing in vulputate ante ullamcorper. Sed eros ante, lacinia et sollicitudin et, aliquam sit amet augue. In hac habitasse platea dictumst.
- Nunc posuere quam at lectus tristique eu ultrices augue venenatis. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Aliquam erat volutpat. Vivamus sodales tortor eget quam adipiscing in vulputate ante ullamcorper. Sed eros ante, lacinia et sollicitudin et, aliquam sit amet augue. In hac habitasse platea dictumst.

1.5. Metodología propuesta

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aliquam ultricies lacinia euismod. Nam tempus risus in dolor rhoncus in interdum enim tincidunt. Donec vel nunc neque. In condimentum ullamcorper quam non consequat. Fusce sagittis tempor feugiat. Fusce magna erat, molestie eu convallis ut, tempus sed arcu. Quisque molestie, ante a tincidunt ullamcorper, sapien enim dignissim lacus, in semper nibh erat lobortis purus. Integer dapibus ligula ac risus convallis pellentesque.

1.6. Distribución de resoponsabilidades para el desarrollo del proyecto

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aliquam ultricies lacinia euismod. Nam tempus risus in dolor rhoncus in interdum enim tincidunt. Donec vel nunc neque. In condimentum ullamcorper quam non consequat. Fusce sagittis tempor feugiat. Fusce magna erat, molestie eu convallis ut, tempus sed arcu. Quisque molestie, ante a tincidunt ullamcorper, sapien enim dignissim lacus, in semper nibh erat lobortis purus. Integer dapibus ligula ac risus convallis pellentesque.

1.7. Resultados esperados

1. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aliquam ultricies lacinia euismod. Nam tempus risus in dolor rhoncus in interdum enim tincidunt. Donec vel nunc neque. In condimentum ullamcorper quam non consequat. Fusce sagittis tempor feugiat. Fusce magna erat, molestie eu convallis ut, tempus sed arcu. Quisque molestie, ante a tincidunt ullamcorper, sapien enim dignissim lacus, in semper nibh erat lobortis purus. Integer dapibus ligula ac risus convallis pellentesque.

2. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aliquam ultricies lacinia euismod. Nam tempus risus in dolor rhoncus in interdum enim tincidunt. Donec vel nunc neque. In condimentum ullamcorper quam non consequat. Fusce sagittis tempor feugiat. Fusce magna erat, molestie eu convallis ut, tempus sed arcu. Quisque molestie, ante a tincidunt ullamcorper, sapien enim dignissim lacus, in semper nibh erat lobortis purus. Integer dapibus ligula ac risus convallis pellentesque.

3. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aliquam ultricies lacinia euismod. Nam tempus risus in dolor rhoncus in interdum enim tincidunt. Donec vel nunc neque. In condimentum ullamcorper quam non consequat. Fusce sagittis tempor feugiat. Fusce magna erat, molestie eu convallis ut, tempus sed arcu. Quisque molestie, ante a tincidunt ullamcorper, sapien enim dignissim lacus, in semper nibh erat lobortis purus. Integer dapibus ligula ac risus convallis pellentesque.

1.8. Actividades y cronograma de trabajo

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aliquam ultricies lacinia euismod. Nam tempus risus in dolor rhoncus in interdum enim tincidunt. Donec vel

nunc neque. In condimentum ullamcorper quam non consequat. Fusce sagittis tempor feugiat. Fusce magna erat, molestie eu convallis ut, tempus sed arcu. Quisque molestie, ante a tincidunt ullamcorper, sapien enim dignissim lacus, in semper nibh erat lobortis purus. Integer dapibus ligula ac risus convallis pellentesque.

1.9. Impactos esperados

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aliquam ultricies lacinia euismod. Nam tempus risus in dolor rhoncus in interdum enim tincidunt. Donec vel nunc neque. In condimentum ullamcorper quam non consequat. Fusce sagittis tempor feugiat. Fusce magna erat, molestie eu convallis ut, tempus sed arcu. Quisque molestie, ante a tincidunt ullamcorper, sapien enim dignissim lacus, in semper nibh erat lobortis purus. Integer dapibus ligula ac risus convallis pellentesque.

Bibliografía

Angraal, Suveen, Harlan M Krumholz y Wade L Schulz (2017). «Blockchain technology: applications in health care». En: *Circulation: Cardiovascular Quality and Outcomes* 10.9, e003800.

Arias, Jordi Cabral (2018). «Estado del arte de la tecnología Blockchain ¿Burbuja o consolidación?» Tesis doct. Universidad oberta de Catalunya.

Banafa, Ahmed. *IC y Blockchain: retos y riesgos*.

Crosby, Michael y col. (2016). «Blockchain technology: Beyond bitcoin». En: *Applied Innovation* 2, págs. 6-10.

Huckle, Steve y col. (2016). «Internet of things, blockchain and shared economy applications». En: *Procedia computer science* 98, págs. 461-466.

Iansiti, Marco y Karim R Lakhani (2017). «The truth about blockchain». En: *Harvard Business Review*.

Kosba, Ahmed y col. (2016). «Hawk: The blockchain model of cryptography and privacy-preserving smart contracts». En: *2016 IEEE symposium on security and privacy (SP)*. IEEE, págs. 839-858.

Nakamoto, Satoshi (mayo de 2009). «Bitcoin: A Peer-to-Peer Electronic Cash System». En: URL: http://www.bitcoin.org/bitcoin.pdf.

Zheng, Zibin y col. (2016). «Blockchain challenges and opportunities: A survey». En: *Work Pap.–2016*.