

Universidad de Costa Rica

Sede Regional del Atlántico

Recinto Turrialba

INFORME DE INVESTIGACIÓN: “Block Chain”

IF-6201 Informática Aplicada a los Negocios.

Profesor: Rolando Herrera Sánchez.

Estudiantes:

Carolina Hernández Campos B3356

Christian Cordero Fallas B72283

Sebastián Gómez Cordero B73220

II Semestre, 2020.

Tabla de contenido	
Contenido	3
Tipos de Blockchain	5
Características	7
Funcionamiento	8
Seguridad de la cadena de bloques	11
Arquitectura de blockchain	12
Ventajas	13
Desventajas	14
Usos	15
Recomendaciones	17
Referencias Bibliográficas	18

1.CONTENIDO

En la sociedad el manejo de la información siempre ha tenido un impacto importante para los seres humanos, actualmente el mundo necesita almacenar y gestionar una gran cantidad de información la cual deber ser veraz y certificada, es decir, no se trata solamente de mantener almacenada la información en algún lugar, sino que es mantener la más pertinente y ver que se hace con ella para darle sentido dentro de las funciones de las empresas. Esta es una de las razones por las cuales han nacido nuevas tecnologías para el manejo de la información, ya que nace de la necesidad del ser humano de hacer los trabajos de manera más eficiente buscando simplificar optimizar sus recursos y simplificar su trabajo.

Desde que nació el internet hasta ahora, han evolucionado una gran cantidad de herramientas útiles para las personas, tanto para uso personal como laboral, además han nacido aplicaciones que son capaces de dar soporte a grandes empresas. El almacenamiento en la nube, medios sociales, el internet de la cosas son solo ejemplos de lo que ha revolucionado con la existencia del internet, además de que le da a las empresas la oportunidad de que la investigación y el manejo de la información sea más sencilla, ya que desde un ordenador se puede acceder fácilmente a los datos requeridos y utilizarlos a conveniencia.

La idea detrás de la tecnología blockchain se describió por primera vez en 1991, por los científicos Stuart Haber y W. Scott Stornetta quienes introdujeron esta tecnología como un registro digital de archivos (de audio, imagen, video o texto) que estuvieran ordenados cronológicamente permitiendo conocer la fecha de su creación así como su autor, entonces surgió como método para almacenar los documentos digitales con sello de tiempo y así evitar que estos pudieran ser modificados o manipulados. En 1992 se incorporaron al diseño los árboles Merkle, estos son como árboles comúnmente conocidos en la informática, son una estructura de datos con la finalidad de relacionar cada nodo con una raíz única asociada donde cada uno de sus nodos posee un identificador único conocido como hash, con la implementación de estos árboles en el modelo blockchain se optimizo ya que permitió colocar varios documentos en un solo bloque pero a pesar de esto esta tecnología no se utilizó y la patente caducó en 2004.

Esta tecnología apareció nuevamente en 2008 con el nacimiento de Bitcoin por Satoshi Nakamoto, creador o grupo de creadores, esta criptomoneda utiliza la tecnología blockchain para proporcionar un método de pago electrónico que no requiere supervisión y evita el control de las instituciones financieras como bancos, entre otros, a pesar del éxito de las criptomonedas con el uso de esta tecnología, blockchain se ha utilizado como una herramienta con múltiples

aplicaciones como: registro de documentos de forma descentralizada, historiales médicos, en registros de propiedad, control de aduanas, sistemas de votación, monitorización de procesos de producción, etc.

Dicho lo anterior y para continuar con el resto del desarrollo es importante conocer el significado de Blockchain y para esto Marcos Allende López (2018) en su documento titulado “Blockchain-Cómo desarrollar confianza en entornos complejos para generar valor de impacto social” menciona que: “El término blockchain, o cadena de bloques en español, se debe a la estructura de esta base de datos, consistente en conjuntos de transacciones que son organizados y almacenados en bloques”(p.5), con la cita anterior queda claro que el blockchain es una cadena o secuencia de un bloque tras otro que almacenan información sobre transacciones, pero en realidad blockchain no es una base de datos porque su propósito principal no es el de almacenar datos si no registrar transacciones, sin embargo se puede utilizar en conjunto con una base de datos para almacenar archivos pesados u otros datos que requieran más espacio.

Como se mencionó anteriormente es una cadena o secuencia de bloques que contienen transacciones y estos están ordenados por orden de llegada, o sea, están ordenados de acuerdo a como vayan surgiendo dichas transacciones y vayan completando el número de transacciones por bloque, cabe destacar que cada uno de los bloques contiene y tienen un número de bloque que es un código alfanumérico llamado hash, una firma digital de la persona encargada de la validación de ese bloque que además es la persona encargada de “encontrar” ese código además de un otro código señalando a su bloque anterior.

Con respecto a los bloques de la cadena se puede mencionar que son de carácter inmutable ya que la única forma de modificar la información contenida en un bloque validado es crear una nueva transacción que se encargue de actualizar la información deseada y de este modo modificarla, cabe destacar que es imposible editar o borrar el contenido de un bloque validado y añadido a la cadena.

1.1.TIPOS DE BLOCKCHAIN

Existen varios tipos de blockchain los cuales se distinguen por sus funcionalidades, protocolos de consenso, reglas para la validación de transacciones y su flexibilidad de administración en la red. A continuación, se describen estos tipos:

-Públicas: Las blockchain públicas es una red descentralizada, a las que todo el mundo tiene acceso. Entre sus características se encuentran que los usuarios son anónimos, además que la seguridad de este tipo de redes está basada en protocolos de consenso para la validación de transacciones. Son redes transparentes y al ser públicas, cualquier usuario puede agregar una transacción siempre y cuando sea válida, así como ver las transacciones usando un explorador de bloques. El proceso para tener o usar una blockchain pública empieza con la descarga de la aplicación correspondiente y hacer la conexión automáticamente con un número de nodos con la versión de la cadena más actualizada, Una vez actualizado el nodo, ya puede realizar transacciones bajo los protocolos establecidos. Los ejemplos más populares de este tipo de blockchain son Bitcoin y Ethereum.

-Privadas: A diferencia de las públicas, estas no están abiertas al público, ya que son cadenas de bloques con permisos, esto quiere decir que solo se puede acceder a ellas mediante invitación. En ellas hay una entidad encargada es la que debe mantener la cadena, asignar los permisos y proponer transacciones, así como aceptar los bloques. Este tipo de tecnología son más utilizadas en el entorno financiero, algunos ejemplos son: Hyperledger, creada por Linux, Ripple el cual es un protocolo que facilita las transferencias monetarias a nivel internacional, R3 la cual es una firma de software empresarial que ofrece tecnología de contabilidad distribuida para las empresas y Universa, es una red descentralizada que ofrece servicio de sistemas de pago interbancario que cualquier empresa puede usar para sus transacciones.

-Híbridas o Federadas: Este tipo es una combinación de las públicas y privadas, a diferencia de las públicas esto no permite que cualquier persona participe del proceso de validación de las transacciones y varias empresas o entidades están a cargo de su administración. Este tipo de tecnología ha surgido de la idea de servir como bases de datos descentralizadas que puedan generar confianza en grandes y complejos entornos, por lo que un determinado número de compañías o entidades se encargan de la administración de la red y ponen a disposición una interfaz web para los usuarios. Algunos ejemplos de este tipo de tecnologías son: Hyperledger, Corda, Quorum.

-Blockchain como un servicio (BasS): Se trata de grandes compañías que venden servicios de almacenamiento de los datos de tu blockchain en la nube, dando la ventaja de que aumente la seguridad, además de un ahorro en costos ya que no hay necesidad de invertir en un hardware. Algunos ejemplos de este son el IBM la cual está especializada en Hyperledger, Microsoft ofreciendo servicios de R3, Hyperledger Fabric o Quorum, entre otras

1.2.CARACTERÍSTICAS

La tecnología de Blockchain tiene algunas características, entre ellas las siguientes:

1. Seguridad: Una de las características más importantes del blockchain es que no se puede modificar ni eliminar nada, solo añadir y esta última lo hace de forma específica, es decir no tan fácilmente haciendo que cada vez que se agrega una transacción no se pueda manipular el sistema de forma deshonesto.
2. Inmutabilidad: Esta es una de las características claves de la tecnología de blockchain ya que es la que nos garantiza que la tecnología se mantenga como ya es, es decir que siga siendo una red permanente y que no se puede alterar. Esto se debe a que dicha tecnología funciona un poco distinta a otras, ya que sus características se mantienen a través de una colección de nodos, en donde cada uno de los nodos tiene una copia del registro digital. Para una nueva transacción cada nodo debe verificar su validez y si la mayoría acepta su validez entonces se agrega al registro.
3. Transparencia: Debido a su funcionamiento de la colección de nodos en donde cada uno verifica su validez, es que se promueve la transparencia, ya que sin la mayoría de los nodos no da su consentimiento no se pueden agregar transacciones al registro. Un ejemplo perfecto para comprobar esta característica, son las blockchain públicas, en las cuales cualquier persona puede observar las transacciones por lo que se garantiza la transparencia.
4. Confianza: A diferencia de las bases de datos tradicionales, blockchain ofrece un protocolo de consenso el cual permite que los distintos no tengan que confiar en los otros, este consenso compartido permite que aún así los nodos puedan compartir un registro de información confiable entre ellos.
5. P2P (Peer-to-Peer) : El manejo de los nodos en blockchain se maneja mediante peer-to-peer, esto quiere decir que no todos los nodos están conectados entre sí, si no que solo está conectado con un número determinado de ellos que se comporten como iguales actuando como servidores y clientes respecto a los demás nodos de la red. De esta forma cuando un nodo quiere informar de una nueva transacción, le envía la información a los nodos que están conectado a él y estos van replicando la información a los que ellos están conectados y así sucesivamente, hasta que la información sea compartida en toda la red.

1.3.FUNCIONAMIENTO

Antes de proceder con la explicación acerca del funcionamiento de esta tecnología es importante aclarar el concepto de transacción, en este contexto una transacción se refiere a cualquier tipo de intercambio de información capaz de ser contenida en un bloque, en general, cualquier información que tenga que ver con la cadena de bloques que queda registrada en un bloque del blockchain en forma de transacción, además a cada uno de los participantes del blockchain son vistos como un nodo que forma parte de la cadena de bloques.

Para explicar el funcionamiento de esta tecnología se utilizarán 6 pasos que se describirán a continuación:

- Paso 0: este paso es por el que se debe pasar para llegar a formar parte de algún blockchain, es decir, ser participante y para esto hay dos opciones dependiendo si se trata de un blockchain de tipo público o privado u híbrido. Si se trata de un blockchain público se debe descargar la aplicación o programa correspondiente para integrarse como un nodo (participante) que posea los mismos privilegios que el resto de los nodos, es decir, cualquiera que quiera puede participar solamente con descargar el software necesario y este a su vez se conectará automáticamente con un número determinado de nodos, pero si se trata de un blockchain de tipo privado o híbrido se accederá a través de una interfaz web que los nodos administradores tengan destinada para el acceso del resto de usuarios autorizados, entonces en la cadena habrán unos nodos privilegiados administrando la cadena y decidiendo cómo un usuario accede a través de la interfaz web.
- Paso 1: Este paso es en el que se envía información en forma de transacciones que posteriormente formarán los bloques de la misma, en pocas palabras, es cuando un nodo quiere realizar una transacción y envía esa información a los nodos con los que tiene conexión, además en este paso entra en acción un primer protocolo que funciona automáticamente en cada uno de los nodos y se comprueba que la información recibida (las transacciones) sean correctas, por ejemplo que no se esté transfiriendo un dinero que no esté en la cuenta, etc. Si la transacción es correcta cada nodo procede a añadirla a su lista de transacciones, llamada pool, y la reenvía a los nodos a los que cada uno de ellos está conectado y así sucesivamente, si a un nodo le llega información sobre una transacción que ya tiene en su lista simplemente ignora esa información.
- Paso 2: En este paso los nodos van llenando su lista de transacciones (pool) con las transacciones que va recibiendo de los otros nodos con los que están relacionados, cabe

destacar que los pools de dos nodos diferentes pueden ser diferentes ya que el orden en el que le llegan las transacciones puede ser distinto.

- Paso 3: En este paso en cada ronda, que puede variar desde unos pocos segundos hasta varios minutos, se escoge aleatoriamente un nodo para proponer un bloque, esto es muy importante ya que es el proceso responsable de que blockchain sea una “base de datos” donde los nodos no tienen que confiar unos en otros, este proceso de selección aleatoria es conocido como protocolo de consenso que se explicará más adelante. Para que el nodo escogido proponga un bloque se toma la versión actual de la cadena de bloques y se le añade al final un bloque que contenga las transacciones que registradas en su pool, luego se envía esta nueva copia de la cadena a los nodos con los que esté conectado el nodo y esos a su vez la enviarán a los que están conectados y así sucesivamente hasta abarcar toda la red resto de la red, esto se hace de igual manera que se hace con cada una de las transacciones, cabe mencionar que los bloques poseen un tamaño máximo de transacciones, este tamaño dependerá del blockchain.
- Paso 4: En este paso el nodo elegido propone un bloque nuevo con las transacciones registradas en su pool pero, antes de ser enviado al resto de los nodos, este bloque debe ser validado con un hash, un código alfanumérico que se obtiene a partir de la información del bloque, más adelante se abordará con más detalle lo referente al hash como su creación, función, etc.
- Paso 5: Aquí es donde los protocolos internos del blockchain acepta el bloque solo si tiene un hash válido, de ser así el resto de nodos verificarán que todas las transacciones también sean correctas y proceden a actualizar su copia de la cadena con esta nueva versión.

Para su funcionamiento, los blockchain cuentan también con protocolos de consenso, como se mencionó anteriormente, es el proceso aleatorio mediante el cual se elige un nodo para que proponga un nuevo bloque, el propósito de esto es que no haya un responsable único de la proposición de bloques, hay diversos procedimientos que se utilizan como protocolos de consenso y a continuación se describirán algunos de los más utilizados como:

- Proof-of-Work (PoW): Este procedimiento corresponde al grupo de protocolos de consenso donde se exige un esfuerzo a los participantes para determinar aleatoriamente quién propone el siguiente bloque y se da una recompensa al ganador, este esfuerzo consiste en utilizar la capacidad computacional (una computadora) que realice intentos aleatorios para encontrar el código hash que valide el bloque, además, cuanto mayor

potencia posea la computadora mayor será la probabilidad de obtener el código válido, esto porque cuando se propone un nuevo bloque este se propone sin un código hash por eso todos los nodos pueden competir por encontrarlo, quienes lo hacen son conocidos como mineros debido a que al proceso de encontrar el código se denomina minar.

- **Proof-of-Stake (PoS):** Este protocolo y los siguientes consisten en asignar mayor probabilidad de ser elegido a aquellos nodos que tienen más activos en la red, aquí no hay nodos compitiendo por validar el bloque y por lo tanto tampoco hay recompensa para quien lo consigue.
- **Leased-Proof-of-Stake (LPoS):** Este es una variación de PoS en la que los nodos con poco capital pueden ceder sus probabilidades de ser elegidos a otro nodo, si el nodo en el que hayan delegado sus probabilidades resulte ganador y haya algún tipo de recompensa por el minado, se reparte proporcionalmente entre el nodo ganador y los que lo apoyaron.
- **Delegated-Proof-of-Stake (DPoS):** Una variación de PoS en la que los nodos pueden proponer a cualquier otro nodo para validar bloques, conocidos como testigos, o para decidir sobre las características, como tiempo entre bloques o tamaño del bloque, de la propia red, que son conocidos como delegados. Cuanto más poder tiene un nodo en la red, más cuenta su voto. Cada nodo propone un número de nodos suficiente como para que se considere suficientemente descentralizada la red, y la elección se repite tras un tiempo establecido.
- **Proof of Importance (PoI):** Este protocolo funciona como PoW pero asignando la probabilidad de ser elegido en función de la actividad como transacciones, balance o reputación en la red del nodo en lugar de su capital, pero se mantiene la idea de premiar con el derecho de proposición de bloques a las personas que más interesadas están en el buen funcionamiento de la cadena, de forma que no les convenga proponer bloques maliciosos que puedan perjudicarla.

1.4.SEGURIDAD DE LA CADENA DE BLOQUES

En cuanto a la seguridad de la cadena es importante mencionar tres puntos. Estos son los siguientes:

-Hash: Se trata del código alfanumérico que se obtiene aplicando una función matemática a un conjunto de datos concatenados, este conjunto de datos es toda aquella información del bloque que se van a encriptar y sobre la cual se quiere detectar cambios. A cada conjunto de datos le corresponde un único Hash y su objetivo es tener la información concatenada de cada bloque en un único código alfanumérico para poder detectar cambios en los bloques con solo mirar el hash. En blockchain se agregan dos piezas más que permiten la seguridad de la cadena, la primer pieza es el código del hash del bloque anterior, para que si hay información alterada en un bloque, el hash de ese bloque y los que lo siguen serán inválidos, así se podrá detectar cualquier cambio en cualquier bloque con solo ver el último bloque. La segunda pieza es el nonce, el cual es un código alfanumérico aleatorio, para que los hashes empiecen con un número de ceros, por lo que para obtener un hash válido este nonce va cambiando de forma aleatoria y se aplica la función hash hasta obtenerlo. Aquí entra en función la minería de datos, en donde los mineros se encargan de probar nonces aleatoriamente hasta tener un hash válido, esto si el protocolo de consenso es PoW.

-Capacidad de rechazar transacciones y bloques inválidos: Cuando un nodo recibe una transacción, lo que se hace es que se revisa que las operaciones sean correctas, es decir que las transacciones sean válidas, de igual forma sucede con los bloques, para que uno sea aceptado todas las transacciones de ese bloque deben ser válidas y tener un hash válido.

-Protocolos de consenso, descentralización y teoría de juegos: Esto permite tener un base de datos distribuida en distintas partes con la seguridad de que la información que traspasan es correcta y que además pueden rechazar la información que no sea veraz.

1.5.ARQUITECTURA DE BLOCKCHAIN

Blockchain debe ser considerada como una herramienta de solución, no como una solución completa. Por lo que una solución además de estar integrada por blockchain también va a tener otras herramientas como interfaz web, que será utilizada en los blockchains de tipo privados y federados, y una bases de datos en la que los documentos pesados serán almacenados.

Pero la arquitectura de esta tecnología se puede definir como una secuencia de bloques donde se almacenan una lista del registro de transacciones, formados por bloques, el primero de ellos se conoce como génesis y es el único que no contiene un hash(referencia al bloque anterior), además contienen una marca de tiempo, un campo nonce (calcula el hash) y la secuencia de transacciones.

1.6.VENTAJAS

Blockchain cuenta con algunos beneficios, cabe destacar los siguientes:

- **Transparencia:** Esto debido a que todos los usuarios del sistema comparten los mismos datos o documentación y solo se pueden actualizar si todos los usuarios se encuentran a favor del cambio ya que al cambiar un solo registro, modificaría todos los registros posteriores. Lo anterior mencionado da confianza de que es una red precisa, consistente y transparente.
- **Alta Disponibilidad:** Blockchain proporciona datos precisos, completos y de fácil acceso, ayudando a acelerar procesos, facilitar la disponibilidad de registros y como objetivo principal ayuda al comercio.
- **Durabilidad, fiabilidad y longevidad:** Blockchain es una gran tecnología para almacenar registros o todo tipo de datos donde cuente con un seguimiento de auditoría, ya que los datos que se registran en la cadena de bloques no pueden ser borrados o cambiados fácilmente y porque todos los cambios son rastreados y registrados permanentemente en un libro de distribución.
- **Reducción en el coste de transacciones:** Esta tecnología provee grandes ahorros en costes de transacción gracias a que solo requiere la confianza de los datos de la cadena de bloques que son transferidos, no es necesario confiar en un socio comercial y que este fue ya anteriormente verificado.
- **Transacciones más rápidas:** Blockchain opera todo el día y los 365 días del año, esto es una razón para que las transacciones sean más rápidas. También, al tener acceso a los datos del sistema todos los usuarios, no se necesitan intermediarios por lo que es fácil confiar en los datos, esta es otra razón por la que las transacciones son muy rápidas.

1.7.DESVENTAJAS

En cuanto a las desventajas que presenta esta tecnología se puede decir que la principal es que se trata de una tecnología actual y revolucionaria por lo que generalmente es muy costosa para las empresas. Otro inconveniente que presenta es porque en su funcionamiento se ejecutan gran cantidad de nodos conectados al mismo tiempo produciendo un gran desperdicio en gastos de energía y tiempo. Con cada transacción de datos esta se agrega a la cadena de bloques que va creciendo y a su vez los requisitos informáticos van aumentando.

Algunas otras desventajas presentes en Blockchain son las siguientes:

- **Anonimidad:** Uno de los defectos que presenta es que al ser una red abierta, cualquier persona puede ver el registro de transacciones tanto pasadas como futuras pero esto aplica solo en el caso de los blockchain públicos donde cualquiera que cuente con el software se pueda unir al mismo.
- **Inmutabilidad de la información:** Como se explicó anteriormente los datos no se eliminan porque es difícil hacerlo, entonces produciría grandes problemas si se ingresan datos incorrectos por parte de algún usuario, ya que no se van a poder modificar o borrar en ese mismo bloque, además para hacer un cambio en la información de algún bloque se debe crear una nueva transacción que lo modifique y esto supone mayor espacio con el simple hecho de realizar un cambio en la información.
- **Desempleo:** Esta tecnología al no usar intermediarios estos se vuelven inútiles, por los que desiste de su uso casi total y conforme pase el tiempo va a aumentar el desempleo de los intermediarios en empresas que implementen blockchain.

1.8.USOS

Los casos de uso de la tecnología de blockchain es muy amplia y revolucionaria, sin embargo, la más conocida es en las cripto-monedas, específicamente en bitcoin. A continuación, se describen algunos otros casos de uso y aplicaciones donde se puede implementar blockchain y recibir ganancias.

Procesos electorales: Como esta tecnología permite la interacción de una gran cantidad de usuarios y es de libre acceso puede ayudar contra el fraude electoral.

ONG: Se podría convertir en la forma más conveniente en mandar de manera eficaz recursos económicos a zonas de difícil acceso por estar en conflictos o afectadas por fenómenos naturales.

Cadenas de suministro: Ayuda a mejorar el seguimiento de la producción y su supervisión. Otras ventajas de la tecnología es que permite que reduzcan costos, ya que permite una mejor trazabilidad y transparencia de los datos, así ayuda a las empresas a identificar las áreas en las que se producen pérdidas y así poner en marcha medidas de ahorro de costos. Así mismo la implementación del blockchain en las cadenas de suministro ayuda a resolver uno de los problemas más comunes en ellas, que es la incapacidad de integrar todos los datos a todos los participantes del proceso, ya que la forma de funcionamiento en la que cada nodo de red contribuye a la inclusión de datos y verificación de su integridad, permite que la información almacenada en la blockchain es accesible a todas las partes involucradas, por lo que es más sencillo para la organización verificar la información que está siendo propagada. Además le da a las empresas beneficios como por ejemplo, la autenticidad y la verificación, la capacidad de resolver problemas y aislarlos para su resolución, no se pueden manipular productos por lo que se permite la transparencia, entre otras.

Ciberseguridad: La tecnología permite que la información almacenada no se pueda modificar o eliminar, debido a su característica de inmutabilidad, por lo que se permite gestionar la información de forma confiable para la seguridad.

Identidad digital: Actualmente el robo de identidad es uno de los más comunes en internet y en las empresas esto puede generar mayores problemas ya que pueden estar en juego muchos datos, también de manera individual es un gran problema, debido que, a la virtualización, los datos personales de una persona pueden estar en internet, desde la dirección del trabajo hasta la cédula de identidad pueden estar ahí. Por lo que tener una identidad digital a través de blockchain le ayuda al individuo a mantener una identidad protegida en toda la red.

Sector de la salud: Puede ayudar en el almacenamiento de registros médicos, ya que actualmente los pacientes llevan sus datos de un médico a otro y los intentos de tener un expediente digital son muy vagos en algunos aspectos por lo que puede generar problemas cuando se trata de recuperación o almacenamiento de datos. La tecnología de blockchain puede simplificar dichos problemas al proporcionar un enfoque descentralizado, en donde todos los interesados puedan acceder a la información del paciente y así sus datos se mantendrán seguros. Además, todas las transacciones se mantendrán en la blockchain por lo que se pueden rastrear cuando sea necesario. Algunos ejemplos de proyectos de blockchain en atención médica son:

-SimplyVital Health – Se basa en dos productos: El primero es ConnectingCare, está diseñado para proveedores de atención médica, como hospitales. Ayuda a estos clientes a optimizar los datos para ahorrar tiempo y dinero. Y el segundo Health Nexus maneja la liquidez, los pagos y el almacenamiento de datos, y está diseñado específicamente para la atención médica

- MediBloc – Mejora de los proveedores de servicios de salud
- Dentacoin – Tiene como objetivo mejorar la atención médica dental.

2.RECOMENDACIONES

Blockchain se encuentra en un crecimiento constante ya que es cada vez más utilizada en diferentes empresas a nivel mundial, tanto que se menciona que en unos años llegará a ser utilizada en más del 50% de las empresas nacionales, todo esto porque los jóvenes cada vez estudian carreras relacionadas a la tecnología. Gracias a esto diferentes sectores de producción apuestan por esta tecnología ya que les provee seguridad, eficiencia, transparencia, disponibilidad, entre otros aspectos. Todo lo anterior para lograr un impacto positivo en la economía, sociedad y a nivel político.

Para saber si blockchain será útil en una empresa es básicamente contemplar si hay necesidad de descentralización, que la información sea de carácter inmutable, que se requiera transparencia, consenso y validación, por lo que se debe saber si será útil cumpliendo con las necesidades descritas anteriormente pero además, hay varios criterios que se deben tomar en cuenta para utilizar este modelo como:

- Se debe tener bien definido el problema para poder plantar una solución, en este caso saber si será útil utilizar blockchain o no.
- Se debe tener bien establecido quién tiene acceso a cierta información o permiso de hacer que para así diseñar con precisión la estructura de los nodos y transacciones.
- Blockchain puede ayudar en donde haya mucha diferencia entre los participantes (gobierno, organización, trabajadores por ejemplo), ya que los consensos deberán ser más complejos y al igual que los clientes las transacciones serán más variadas.
- En cuanto al presupuesto no se puede estimar un presupuesto general sobre el costo de una solución utilizando blockchain, ya que las posibles implementaciones son muy diversas y además blockchain no está pensado para soluciones a pequeñas escalas.

3. REFERENCIAS BIBLIOGRÁFICAS

Allende, M. (2018). Blockchain-Cómo desarrollar confianza en entornos complejos para generar valor de impacto social. Recuperado de:

<https://www.hacienda.go.cr/Sidovih/uploads//Archivos/Articulo/Blockchain.pdf>

Dolader, C., Bel, J., Muñoz, J. (s,f).La blockchain: Fundamentos, aplicaciones y relación con otras tecnologías disruptivas. Recuperado de:

<https://www.mincotur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/405/DOLADER,%20BEL%20Y%20MU%C3%91OZ.pdf>

ESIC Business & Marketing School (2018). Blockchain: la guía definitiva para conocer esta tecnología. Recuperado de: <https://www.esic.edu/rethink/tecnologia/blockchain-la-guia-definitiva>

Master Ethereum (2018). Ventajas y desventajas del uso de Blockchain. Recuperado de:

<https://masterethereum.com/ventajas-desventajas-blockchain/>

Pereira, M (2019). Plataformas blockchain y escenarios de uso. Recuperado de:

<https://www.colibri.udelar.edu.uy/jspui/bitstream/20.500.12008/20541/1/tg-pereira-toscano-villar.pdf>

Vector iTC (2018). Blockchain: disrupción, valor y seguridad. Recuperado de:

<https://www.vectoritcgroup.com/wp-content/uploads/2018/06/Blockchain-Disrupci%C3%B3n-valor-y-seguridad.pdf>