

Blockchain: El auge de las transacciones

Martha Eliana Arenas Márquez
Escuela de ingeniería de sistemas e informática
Universidad Industrial de Santander
elianaarenasm@gmail.com

Carlos Daniel Barrera Manrique
Escuela de ingeniería de sistemas e informática
Universidad Industrial de Santander
cbarreram99@gmail.com

Luis Gerardo Castellanos Vergaño
Escuela de ingeniería de sistemas e informática
Universidad Industrial de Santander
luisgecas_78@hotmail.com

Yann Karlo Castellanos conguta
Escuela de ingeniería de sistemas e informática
Universidad Industrial de Santander
yannkarlo@gmail.com

Resumen- *El Blockchain es la tecnología que está implícita en la implementación o desarrollo de la criptomoneda, grandes plataformas principalmente la criptomoneda llamada bitcoin, esta tecnología ha llevado las monedas informáticas a otro nivel, debido a sus propiedades seguras y amigables para el usuario, La principal característica del Blockchain es la integridad y seguridad de los datos, beneficios fundamentales a la hora de trabajar con valores monetarios, además la implementación de firmas digitales fue uno de los factores que llevó al Blockchain a tener el auge que tiene, y el éxito que llevará a un futuro.*

Abstract— Blockchain is the technology implied in development and implementation of cryptocurrency. Big platforms, mainly the one behind Bitcoin has lead digital commerce to a huge new level due to its properties like security and user friendly interface. Blockchain's main feature is integrity and data security when working with currency, also digital signature's implementation was one of the factors that took blockchain to the top and perhaps will secure its success in the future.

I. INTRODUCCIÓN

En la actualidad, hablar de la criptomoneda es algo muy usual, ha tenido tanto impacto en el mercado global que se ha tenido que pensar en nuevas estrategias para proteger los datos que estas plataformas informáticas manejan, actualmente, existen más de 2.000 tipos de criptodivisas, siendo las de

mayor auge en estos tiempos, el bitcoin, el Ethereum, el XRP, entre otras divisas, debido a la gran demanda de la criptomoneda, se llegó a crear el Blockchain, el cual es una técnica de manejo de estas divisas, cuyo objetivo es dar soporte a las plataformas de manejo de criptomoneda, el Blockchain cuenta con formatos, que permiten confidencialidad en los datos, además de implementar una nueva forma de almacenamiento, llamado Versum, el cual puede manejar grandes cantidades de información, asegurando una respuesta correcta, Blockchain también cuenta con la implementación de una clave privada y una clave pública, para garantizar un margen de error del 0% en la realización de transacciones de valor monetario, ofreciendo confiabilidad a los usuarios; además la técnica del Blockchain se puede aplicar a cualquier método que quiera transferir información de un origen a un destino, por esto la mayoría de plataformas pueden hacer uso de esta tecnología para hacer más seguro y fiable su sitio o portal web.

II. ESTADO DEL ARTE

Blockchain es una herramienta que no necesita una autoridad ya que es descentralizado, ofreciendo seguridad e inmutabilidad en los datos.

En la actualidad existen varias aplicaciones de Blockchain donde cada una es diferente y se usa en casos diferentes. La más famosa es la de las criptomonedas como bitcoin. Blockchain tiene otros usos aparte de la criptomoneda, en el sector público donde el uso de esta tecnología posibilita transparencia, participación y privacidad, se usa igualmente en el registro y verificación de datos; en el cual se almacena cualquier tipo de información, generando así un registro distribuido e inalterable. Se ha investigado también sobre el voto electrónico mediante Blockchain, uso en smart contracts, de la misma forma su implementación en el seguimiento de la cadena de suministros, gestión de identidades, seguros entre otras aplicaciones significativas.

Las aplicaciones de Blockchain son muchas y diversas, esta herramienta permite transformar gran parte del mundo y la vida cotidiana dando el control a las personas. Pero así como tiene sus beneficios también presenta algunos desafíos y riesgos en:

- **Regulación y legalidad:** Los gobiernos están vigilantes pero preocupados ante cómo actuar con esta tecnología, donde el principal desafío es conseguir un equilibrio entre regular lo suficiente para evitar usos fraudulentos y no regular demasiado para atraer innovación e inversión.
- **Escalabilidad:** Con el aumento de las transacciones, cada vez la cadena de bloques se hace más grande donde cada nodo tiene que almacenar todas las transacciones para validarlas. Con la cadena de bloques de bitcoin solo se pueden hacer 7 transacciones por segundo, por lo tanto no se cumple con los requisitos de procesar millones de transacciones en tiempo real.
Para mejorar la escalabilidad se ha tratado de optimizar el almacenamiento en Blockchain a partir de una red que elimina y olvida los registros de transacciones anteriores, usando una base de datos llamada árbol de cuentas el cual se utiliza para mantener el saldo de todas las direcciones no vacías. Igualmente se ha rediseñado Blockchain con bitcoin next generation, la idea principal es desacoplar el bloque convencional en 2 partes. El bloque clave para la elección del líder y el microbloque para almacenar transacciones.
- **Privacidad y seguridad:** Blockchain permite cierta cantidad de privacidad a través de la clave pública y privada, a partir de estas los usuarios realizan transacciones sin ninguna exposición de la verdadera identidad. Pero no se puede garantizar la privacidad transaccional ya que los valores de todas las transacciones y saldos de la clave pública son visibles.

III. ARQUITECTURA BLOCKCHAIN

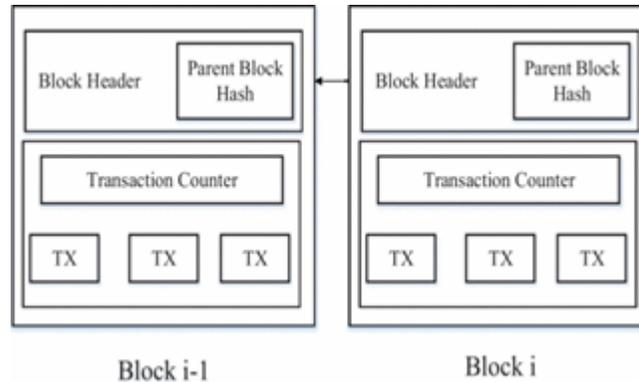


Fig 1. Secuencia de bloques.

Blockchain contiene información específica como una base de datos, agrupado en una red peer to peer (de igual a igual). Este libro mayor distribuido proporciona transparencia, confianza y seguridad de datos. Están enlazados y cifrados para proteger la seguridad y privacidad de las transacciones, que elimina los intermediarios, descentralizando toda la gestión. La arquitectura permite que la información digital se distribuya.

En la arquitectura de Blockchain, cada participante dentro de la red mantiene, aprueba y actualiza las nuevas entradas. Cada miembro se asegura de que todos los registros y procedimientos estén en orden, garantizando validez y seguridad. En otras palabras, Blockchain son computadoras conectadas entre sí en lugar de un servidor central, lo que significa que toda la red está descentralizada.

Estos son los principales componentes de la arquitectura Blockchain:

- **Nodo:** Usuario o computadora que conforma la arquitectura.
- **Transacción:** Bloque de construcción más pequeño de un sistema de Blockchain (registros o información).
- **Bloque:** Es una estructura de datos para mantener un conjunto de transacciones que se distribuye a todos los nodos de la red.
- **Cadena:** Secuencia de bloques en un orden concreto.
- **Mineros:** Nodos específicos que realizan el proceso de verificación de bloques antes de agregar algo a la estructura de la cadena de bloques.
- **Protocolos de consenso:** Reglas y acuerdos para realizar las operaciones de Blockchain.

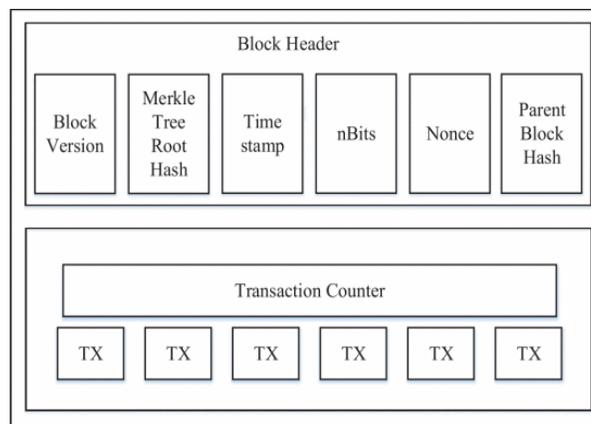


Fig 2. Estructura del bloque

La estructura del bloque está conformada por el encabezado del bloque y el cuerpo del bloque. El encabezado está compuesto por:

- **Versión del bloque:** Contiene la versión del software que ha generado el bloque.
- **Hash de raíz de árbol Merkle:** Valor hash de todas las transacciones en el bloque.
- **Marca de tiempo:** La hora de generación del bloque en formato timestamp.
- **Nbits:** Umbral objetivo de un hash de bloque válido.
- **Nonce:** campo de 4 bytes, generalmente comienza con 0 que incrementa itera
- **Hash:** Puntero codificado, que enlaza el bloque anterior.

En el cuerpo del bloque se encuentra un contador de transacciones, el número de dichas transacciones dependen del tamaño del bloque y tamaño de la transacción. Para autenticar transacciones Blockchain usa criptografía asimétrica.

Las transacciones deben ser seguras para ello, es necesario el uso de firma digital, verificando que las personas que las realicen sean quien dice ser. La firma digital Blockchain usa el algoritmo de curva elíptica, los usuarios deben tener cada uno una clave pública y una privada, donde se usan dos fases: la fase de firma y la fase de verificación. En la fase de firma se usa la clave privada para cifrar los datos y en la fase de verificación se valida el valor con la clave pública.

Blockchain tiene unas características principales: Es descentralizado, persistente anónimo y auditable.

Descentralizado: A partir de los algoritmos de consenso permite que Blockchain mantenga la consistencia de los datos en una red distribuida.

Persistente: Las transacciones se pueden validar, las no válidas no serían admitidas.

Anónimo: La interacción con bloques de una dirección la cual no revela la identidad real del usuario.

Auditable: las transacciones pueden ser fácilmente verificadas y rastreadas.

Los sistemas de Blockchain son de 3 tipos: Blockchain público, Blockchain privado y Blockchain de consorcio.

Al realizar los procesos de consenso, la cadena de bloques públicos todos los registros son visibles y todos pueden participar en el proceso de consenso. En la cadena privada solo podrán participar los nodos que provienen de una organización específica, la cadena de consorcio participan algunos nodos preseleccionados.

Las cadenas públicas son descentralizadas, las privadas centralizadas, la cadena de consorcio es parcialmente centralizada. Al alterar las transacciones es casi imposible modificarlas en una cadena pública ya que los registros se almacenan en muchos participantes. Lo que es contrario en la cadena privada y la cadena de consorcio ya que no hay muchos participantes. Como se ha dicho anteriormente en una cadena pública existen una gran cantidad de participantes por lo tanto su eficiencia en cuanto rendimiento y latencia es peor al compararlas con las cadenas de consorcio y las privadas. En la tabla 1 se puede ver la comparación entre los distintos sistemas de Blockchain.

Propiedades	Blockchain público	Blockchain de consorcio	Blockchain privado
Determinación consenso	Todos los mineros	Nodos seleccionados	Una organización
Permiso de lectura	Público	Público o restringido	Público o restringido
Inmutabilidad	Imposible modificar	Puede ser modificable	Puede ser modificable
Eficiencia	Baja	Alta	Alta
Centralizado	No	Parcial	Si
Proceso de consenso	Sin permiso	Autorizado	Autorizado

Tabla 1. Comparación entre Blockchain público, de consorcio y privado.

IV. ALGORITMOS DE CONSENSO

Lograr un acuerdo en un ambiente distribuido como la red de Blockchain es todo un reto. Se necesitan protocolos para asegurar que las cuentas en los diferentes nodos son consistentes.

- **ACERCAMIENTOS AL ACUERDO:**

- **Prueba de trabajo (Pow):** En una red descentralizada alguien tiene que seleccionarse para registrar las transacciones. Se hace al azar pero esta forma es vulnerable a ataques.

En este protocolo a cada nodo de la red se le calcula un valor hash de la cabecera de bloque (block header). Esta contiene un anuncio y los mineros lo cambian frecuentemente para obtener diferentes valores hash. El consenso requiere que el valor calculado sea igual o menor que un valor dado. Cuando un nodo alcanza el valor especificado, se transmite el bloque a otros nodos y estos nodos confirmarán mutuamente la exactitud del valor hash. Si el bloque se valida, otros mineros agregarán este nuevo bloque a sus propias Blockchain. Los nodos que calculan los valores hash se llaman *mineros* y el procedimiento de la Prueba de Trabajo se llama *minería* de *Bitcoin*.

La desventaja de este protocolo es que los mineros tienen que hacer muchos cálculos computacionales en PoW, lo que gasta muchos recursos.

Bitcoin usa un servidor de marcas de tiempo distribuido entre pares para generar una prueba computacional de orden cronológico en las transacciones. El sistema es seguro en la medida en que los nodos honestos controlan de forma colectiva mejor el poder de la CPU que otros grupos de nodos cooperativos atacantes.

La Prueba de trabajo involucra escanear un valor que una vez hasheado, este comienza con un número de cero bits. El trabajo promedio requerido es exponencial al número de cero bits requerido y puede ser verificado ejecutando un solo hash.

Para la red de marcas de tiempo, se implementó La Prueba de trabajo incrementando un nonce en el bloque hasta que un valor que se encuentre nos da al hash del bloque los cero bits. Una vez que el esfuerzo de la CPU se ha gastado para satisfacer la Prueba de trabajo, el bloque no se puede cambiar sin rehacer el trabajo. Al agregar bloques a la cadena, el trabajo para cambiar el bloque incluiría rehacer todos los bloques después de este.

El funcionamiento de la red es el siguiente:

- Las transacciones nuevas se transmiten por todos los nodos.
- Cada nodo agrupa nuevas transacciones en un bloque.
- Cada nodo trabaja en encontrar una dificultad de PoW para su bloque.
- Cuando un nodo encuentra una PoW, transmite el bloque a todos los nodos.
- Los nodos aceptan el bloque solo si las transacciones en él son válidas y no se han gastado.
- Los nodos expresan su aceptación del bloque trabajando en crear el siguiente bloque de la cadena, usando el hash del bloque aceptado como el hash anterior.

Los nodos siempre consideran la cadena más larga como la correcta y seguirán extendiéndola. En el caso de que dos nodos transmitan diferentes versiones del siguiente bloque de manera simultánea, algunos nodos recibirán una, los otros la otra, pero en este caso, los nodos trabajarán en la primera que hayan recibido, y guardarán la otra ramificación en el caso de que se vuelva más larga. El vínculo se cortará cuando la siguiente Prueba de trabajo se encuentre y una ramificación se vuelva más larga. Los nodos que estaban trabajando en la otra ramificación se cambiarán a la más larga.

Existe un incentivo que se da a los nodos para que apoyen la red: la primera transacción en un bloque es especial porque inicia una nueva moneda propiedad del creador del bloque. El incentivo también puede motivar a los nodos a mantenerse honestos.

Es posible verificar pagos sin correr toda la red de un nodo. Un usuario solo necesita conservar una copia de los encabezados del bloque con la cadena de Prueba de trabajo más larga, la cual puede obtener interrogando a los nodos de la red hasta que se convence de que tiene la cadena más larga, y obtiene la ramificación enlazando la transacción al bloque en el que está la marca de tiempo. Este usuario no puede verificar la transacción por sí mismo, sino que tiene que enlazarla a un lugar de la cadena, donde podrá ver que un nodo de la red la ha aceptado, y los bloques añadidos después de ella podrán confirmar posteriormente que la red la ha aceptado.

Si bien es posible manejar las monedas individualmente, sería pesado hacer transacciones separadas para cada céntimo en una transferencia. Es por esto que para permitir que un valor se divida y se combine, las transacciones contienen múltiples entradas y salidas. Normalmente habrá o una simple entrada de una transacción previa grande, o múltiples entradas combinando cantidades más pequeñas, y al menos dos salidas: una por pago, y otra retornando el cambio, si es que lo hay, al remitente [3].

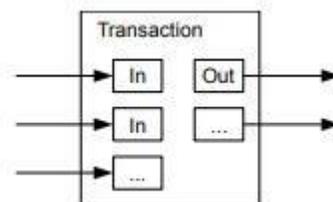


Fig 3. Esquema de una transacción.

- **Prueba de estaca (PoS):** Es una alternativa que ahorra energía a diferencia de Pow. Los mineros en PoS tienen que probar la propiedad de la cantidad de moneda, y se cree que la gente con más tipos de moneda son menos propensos a atacar la red. La selección basada en el balance de cuenta es un poco injusta porque la persona más rica estará obligada a ser dominante en la red.

La desventaja es que como el coste de minar es casi nulo, los ataques no se hacen esperar. Es por esto que al principio las Blockchain empiezan con PoS y gradualmente se pasan a PoW.

- **Tolerancia práctica a fallas bizantinas (PBFT):** Este algoritmo maneja 1/3 de réplicas maliciosas bizantinas. Un nuevo bloque se determina en una ronda. El bloque elegido según ciertas reglas es responsable de ordenar la transacción. Todo el proceso se puede dividir en tres fases; *pre-preparado*, *preparado* y *compromiso*. En cada fase, un nodo pasará a la siguiente si este ha recibido votos de más de 2/3 de los demás nodos. PBFT requiere que cada nodo se conozca en la red.
- **Prueba de estaca delegada (DPOS):** La diferencia con Pos es que DPOS es una democracia representativa, es decir, las partes interesadas eligen a sus delegados para generar y validar bloques. Se reducen los bloques y esto aumenta la rapidez de las transacciones. Algunos parámetros como el tamaño del bloque y los intervalos del mismo los ajustan los delegados.
- **Ripple:** utiliza subredes colectivas confiables dentro de una red más grande. En esta red, los nodos se dividen en dos tipos, servidor (participa en el proceso de consenso) y cliente (transfiere los fondos). Cada servidor tiene una lista única de nodos (UNL) sobre los cuales hará consultas para determinar si poner o no una transacción en el “libro de contabilidad”. Si los acuerdos recibidos alcanzan un 80%, la transacción se empaqueta en el libro. Para un nodo, el libro se mantendrá correcto mientras que el porcentaje de nodos defectuosos sea menor al 20%.
- **Tendermint:** Es un algoritmo de consenso bizantino. Un bloque nuevo se determina en una ronda. Una oferta se selecciona para transmitir un bloque no confirmado en esta ronda. Se divide en tres pasos; pasó de pre voto en donde los validadores escogen si transmitir un prevoto para el bloque ofertado. Paso de pre compromiso, en donde si un nodo ha recibido más de 2/3 de pre compromisos, entra en el paso tres que es el de compromiso en donde el nodo valida el bloque y transmite un compromiso para ese bloque. Si el nodo ha recibido 2/3 de los compromisos, acepta el bloque.
La diferencia con PBFT es que los nodos tienen que bloquear sus monedas para volverse validadores, en la tabla 2, se resumen las diferencias entre cada protocolo/algoritmo.

Propiedad	PoW	PoS	PBFT	DPOS	Ripple	Tendermint
Administración de la identidad del nodo	Abierta	Abierta	Autorizado	Abierta	Abierta	Autorizado
Ahorro de energía	No	Parcial	Sí	Parcial	Sí	Sí
Poder tolerado del adversario	<25% de poder de cómputo	<51% de estaca	<33.3% de réplicas defectuosas	<51% de validadores	<20% de réplicas defectuosas en UNL	<33% de poder de votación bizantina
Ejemplo	Bitcoin	Peercoin	Hyperledger Fabric	Bitshares	Ripple	Tendermint

Tabla 2. Comparación entre protocolo/algoritmo

V. AVANCES FUTUROS DEL BLOCKCHAIN

Se proyecta un gran avance para la tecnología del Blockchain en el mercado global, debido a su técnica de manejo de datos, se espera que se posicione como estándar en los nuevos dispositivos, plataformas y artefactos; el principal campo en el que desempeñará esta tecnología es en el dinero descentralizado, se pretende que los bancos modifiquen su forma de interacción monetaria, disminuyendo así la participación de los bancos a la hora de manejar las finanzas, otra área es la información sensible de gobierno, esto debido a la capacidad de almacenar los datos sin perder ni un bit en el almacenamiento, el internet de las cosas también tendrá esta técnica, ya que deberá estar conectado a la red y se pretende que estos artefactos tomen decisiones autónomas, en los que el hombre tenga la menor intervención posible.

En los próximos meses serán importantes para las tecnologías y aplicaciones que usan y aprovechan Blockchain y el bitcoin, que parecen estar listas para tener un impacto real en el mercado. La carrera global por la regulación del sector en 2019 verá un primer punto de llegada, pero para una adopción sustancial y un impacto concreto en la vida diaria será decisivo para superar los riesgos relacionados con la fluctuación de las criptomonedas, para demostrar la compatibilidad con los nuevos estándares de protección de datos. Introducido por el GDPR (Reglamento general de protección de datos) y resolver el dilema de la escalabilidad.

Con un nuevo año por delante es hora que las cadenas de bloque supere definitivamente el concepto de tecnología en el centro de las monedas virtuales y supere el escepticismo sobre la volatilidad. En realidad, las tecnologías de registro distribuido (denominadas Tecnologías de libro mayor distribuido o DLT) pueden tener numerosas aplicaciones que están completamente desconectadas de las criptomonedas, ya que ofrecen un enfoque totalmente diferente para almacenar información, realizar funciones y ejecutar transacciones, todo ello creando vínculos de fidelidad innovadores, constantes y eficaces.

Los eventos de generación de tokens, las ofertas iniciales de criptomoneda continuarán proliferando, a medida que aumenten la conciencia de los inversores y la atención del gobierno, los métodos de recaudación de fondos basados en Blockchain se harán más sofisticados y maduros.

Se espera que tenga un efecto positivo en los gobiernos y en las posibilidades concretas de adoptar tecnología: los gobiernos dejarán de considerar la cadena de bloques (simplemente) como la tecnología detrás de bitcoin, sino como una oportunidad para mejorar y progresar para ser explotados. Por ejemplo, Suiza, Japón y Canadá ya están realizando las primeras pruebas para adoptar sistemas de votación electrónica basados en Blockchain, para garantizar el secreto de la votación y al mismo tiempo acelerar la verificabilidad de los resultados.

Impulso legislativo para aprovechar las oportunidades del Blockchain:

En general en la mayoría de los principales países el 2018 fue un año de prueba para establecer cómo mejorar las tecnologías basadas en registros distribuidas detrás de las cadenas de bloques y para explorar qué problemas podrían resolverse en realidad, cambiando así los proveedores de tecnología de Prueba de Concepto (POC) a productos y servicios reales.

Las pruebas han demostrado que las aplicaciones basadas en Blockchain pueden reducir efectivamente los costos intermedios entre las partes involucradas en las transacciones y permitir el intercambio de valores entre pares que pueden empoderar y empoderar a los consumidores, superando los modelos tradicionales de control centralizado. y la mejora de los servicios en una amplia gama de sectores clave, como la energía, la salud, los servicios financieros, la gestión de la cadena de suministro, el transporte, la educación y los servicios públicos.

VI. DISCUSIÓN

Para poder ajustar la tecnología Blockchain en Colombia debemos tener en cuenta, el hardware y software necesario. Hablando en términos del software, específicamente de los algoritmos de consenso disponibles en el entorno computacional, inicialmente se debería considerar que la aplicación diseñada use el algoritmo de Prueba de estaca (PoS) para crecer en el mercado, dado que el hardware necesario para minar datos será considerablemente menor, en comparación con el necesario sobre el que trabaja el algoritmo de Prueba de Trabajo (PoW), pero que gradualmente (es decir, a medida que la empresa propietaria de la aplicación logre un posicionamiento en el mercado, teniendo esto como consecuencia mayor poder adquisitivo, y por lo tanto mayor inversión en hardware y software) será viable combinar estos dos algoritmos, como en el caso de Peercoin[9].

En cuanto al usuario debe contar una arquitectura de hardware suficientemente fuerte, para soportar la minería necesaria para construir los bloques de transacciones, de tal forma que no haya inconvenientes en cuanto a sobrecarga de tareas, obteniendo transacciones más eficientes. El bitcoin es una criptomoneda que a nivel mundial está generando desarrollo, tomando cada vez más relevancia, es por esto que el gobierno debe ajustar sus políticas legislativas, para así poder dar paso a esta nueva tecnología en el interior país, para así poder avanzar a un país con mayor desarrollo e innovador,

VII. CONCLUSIONES

- ❖ El Blockchain es una técnica bastante confiable, que garantiza la seguridad y la integridad de los datos, además que cuenta con un almacenamiento tan exacto, que no se pierde ni un solo bit de la información.
- ❖ Bitcoin ha sido de las primeras plataformas en incorporar esta tecnología en el movimiento de su criptomoneda, haciendo su sitio más seguro, aumentando la confiabilidad de los usuarios al mantener divisas en su sitio.
- ❖ La arquitectura detrás de Bitcoin hace uso de una red entre pares, que a su vez usa la Prueba de trabajo para hacer un registro público de las transacciones, que rápidamente se vuelve computacionalmente impráctico de cambiar para un atacante siempre y cuando los nodos honestos controlen una mayoría del poder de la CPU.
- ❖ Los demás algoritmos de consenso ofrecen sus ventajas y desventajas, de cierta forma logrando un balance y siendo adecuados dependiendo de las necesidades de la empresa y su infraestructura de TI.

VIII. REFERENCIAS

- [1] Burgwinkel, Daniel. (2017). [Type of medium]. *volumen (issue)*. Available: Blockchain Technology : Einführung für Business- und IT Manager(3th edition)
- [2] Blockchain (technology). De: Biscontini, Tyler, Salem Press Encyclopedia of Science, 2018 Available: <http://eds.b.ebscohost.com/eds/detail/detail?vid=1&sid=96218537-1f06-4b55-9852-9a7ba5daa1dd%40sessionmgr120&bdata=Jmxhbmc9ZXMmc2l0ZT1lZHMtbGl2ZQ%3d%3d#AN=129815412&db=ers>
- [3] Bitcoins: Tecnologia Blockchain, available: <https://bitcoin.org/bitcoin.pdf>
- [4] Futuro del Blockchain, available: <https://www.lavanguardia.com/economia/management/20181018/452412796056/blockchain-tecnologia.html>
- [5] Blockchain: una tecnologia de exactitud, available: <https://www.xataka.com/especiales/que-es-blockchain-la-explicacion-definitiva-para-la-tecnologia-mas-de-moda>
- [6] El Blockchain en colombia, available: <https://www.meetup.com/es/Blockchain-Colombia/>
- [7] Estrategias del Blockchain, available: <https://www.strategie.gouv.fr/sites/strategie.gouv.fr/files/atoms/files/fs-rapport-blockchain-21-juin-2018.pdf>
- [8] Diferencias en algoritmos de concenso en el Blockchain, available: <https://www.bbva.com/en/difference-dlt-blockchain/>