Cadena de Bloques, Contratos Inteligentes y Criptomoneda.

Murrieta Villegas Alfonso (315048937), Reza Chavarría Sergio Gabriel(315319077) ,
Valdespino Mendieta Joaquín (315115501), Morales González Luis Javier((314108726),
Santillan Godinez Alan Alejandro (315158391)
Universidad Nacional Autónoma de México, Facultad de Ingeniería
CDMX, México

***Abstract*--** Business runs on information. The faster it's received and the more accurate it is, the better. Blockchain is ideal for delivering that information because it provides immediate, shared and completely transparent information stored on an immutable ledger that can be accessed only by permissioned network members. A blockchain network can track orders, payments, accounts, production and much more, through technologies such as smart contracts. Also, members share a single view of the truth, you can see all details of a transaction end-to-end, giving you greater confidence, as well as new efficiencies and opportunities.

I. Introducción

El blockchain como tecnología y como herramienta es sin duda la mayormente compartida e inmutable que facilita el proceso de registro de transacciones y seguimiento de activos en una red empresarial. Pero para poder entender eso, debemos partir que, en este contexto de sistemas distribuidos, un activo puede ser tangible (una casa, automóvil, efectivo, terreno) o intangible (propiedad intelectual, patentes, derechos de autor, marca).

Prácticamente cualquier cosa de valor se puede rastrear y comercializar en una red blockchain, lo que reduce el riesgo y los costos para todos los involucrados.

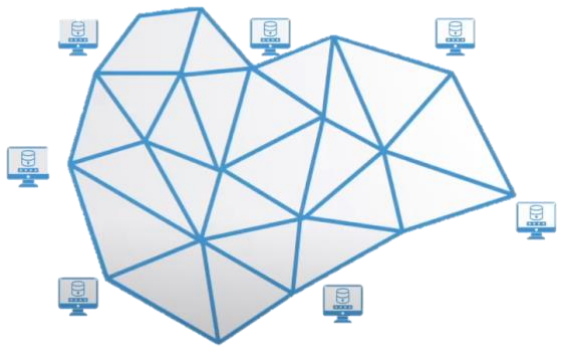

Imagen 1: Distribución de datos en un sistema no descentralizado (Principio básico de un blockchain)

Por otro lado, debemos partir de definir la importancia y qué es como tal el blockchain debido a que tanto los contratos inteligentes como las criptomonedas son una derivación o específicamente subtecnologías que dependen directamente del blockchain.

Hoy en día todos los negocios funcionan con información, y mientras más rápido se reciba y más precisa sea, mejor es la forma de hacer crecer un negocio. Blockchain es ideal para entregar esa información porque proporciona información inmediata, compartida y completamente transparente almacenada en una cadena de contabilidad inmutable al que solo pueden acceder los miembros de la red autorizados.

Una cadena de bloques o blockchain puede rastrear pedidos, pagos, cuentas, producción y muchas más cosas. Y debido a que los miembros comparten una visión única de la verdad, puede ver todos los detalles de una transacción de un extremo a otro, lo que brinda mayor confianza, así como nuevas eficiencias y oportunidades al trabajar de esta forma.

II. Desarrollo

A. Cadena de Bloques o Blockchain

De manera general una cadena de bloques es una grabación digital del historial de transacciones. Sin embargo, blockchain tiene varias características que lo distinguen de un "*libro mayor digital tradicional*" o una "*base de datos relacional*":

- Las cadenas de bloques se distribuyen y gestionan mediante redes de dispositivos informáticos de igual a igual.
- Los datos de las transacciones se comparten entre los participantes de la red blockchain, lo que elimina la necesidad de conciliar libros de contabilidad dispares.

- Una transacción se agrega a la cadena de bloques solo después de haber sido validada a través de un mecanismo de consenso que garantiza que es la única versión de la verdad.

- Los datos son inmutables porque cada transacción está protegida criptográficamente y vinculada a la transacción anterior a medida que se registra.

- Un activo en una cadena de bloques tiene procedencia porque los participantes pueden ver de dónde viene y cómo ha cambiado su propiedad con el tiempo.

1) *Elementos de un Blockchain*

Dentro de una cadena de bloques o blockchain hay varios elementos que comúnmente podemos observar independientemente del objetivo con el que se quiera realizar o emplear un blockchain:

1. *Tecnología de contabilidad distribuida*

Todos los participantes de la red tienen acceso al libro mayor distribuido y su registro inmutable de transacciones. Con este libro mayor compartido, las transacciones se registran solo una vez, lo que elimina la duplicación de esfuerzos que es típica de las redes comerciales tradicionales.

2. *Registros inmutables*

Ningún participante puede cambiar o alterar una transacción después de que se haya registrado en el libro mayor compartido. Si un registro de transacción incluye un error, se debe agregar una nueva transacción para revertir el error, y ambas transacciones serán visibles.

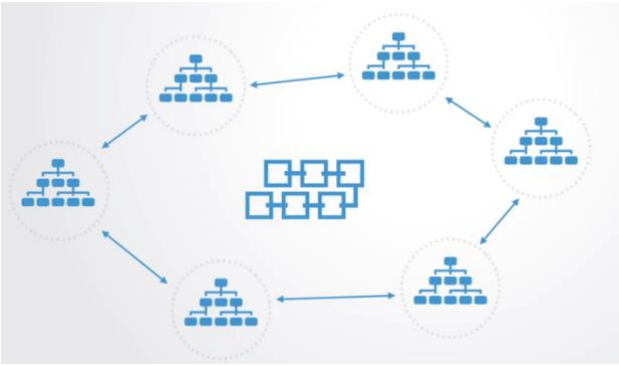

Imagen 2: Al realizar un registro que no puede mutar independientemente de donde esté alojado, esto hace precisamente que nuestra cadena sea segura al momento de realizar transacciones

3. *Contratos inteligentes*

Para acelerar las transacciones, un conjunto de reglas, llamado ***contrato inteligente***, se almacena en la cadena de bloques y se ejecuta automáticamente. Un contrato inteligente puede definir las condiciones para las transferencias de bonos corporativos, incluir términos para el pago del seguro de viaje y mucho más.

2) *Blockchain públicos y privadas*

Desdes que comenzó el blockchain, una de las principales promesas de la tecnología fue la descentralización. Sin embargo, a medida que el espacio maduró, muchos han llegado a reconocer que debe haber compensaciones en la práctica, incluso calificando la descentralización como un mito. Ninguna empresa puede estar completamente centralizada o descentralizada sin comprometer otra área como la seguridad, la privacidad, el rendimiento o la escalabilidad.

Esta es una consideración importante al determinar el mejor enfoque de blockchain para su caso de uso. Es posible que haya escuchado la distinción entre cadenas de bloques públicas y privadas, a veces también caracterizadas como sin permiso y con permiso. Comprender las diferencias entre las cadenas de bloques públicas y privadas es crucial para comprender el tipo de compensaciones que puede necesitar considerar al desarrollar una solución de cadena de bloques.

Tanto las cadenas de bloques públicas como las privadas se basan en alguna forma de tecnología de contabilidad distribuida, pero divergen en cinco áreas clave: permisos, consenso, seguridad, rendimiento y escalabilidad.

1. *Permisos*

En la mayoría de los casos, cualquiera puede participar en una cadena de bloques sin permiso. Los participantes no necesitan cumplir criterios predeterminados ni proporcionar ninguna información sobre sí mismos, y pueden interactuar en la red sin revelar su identidad, utilizando un seudónimo o una dirección alfanumérica. Sin embargo, las transacciones registradas en una cadena de bloques pública son visibles para todos los demás participantes.

El tipo de apertura y seudonimato que existe en una cadena de bloques pública generalmente no es adecuado para transacciones entre entidades comerciales. Por numerosas razones, incluidas **cuestiones normativas** y de **seguridad**, la mayoría de las organizaciones necesitan saber con quién están tratando y también deben asegurarse de que los participantes no autorizados no puedan acceder a los datos de transacciones, que podrían contener información corporativa confidencial.

Incluso dentro del mundo de las cadenas de bloques privadas, es importante considerar qué grado de privacidad es necesario y útil.

Por ejemplo, una cadena de bloques estrictamente privada, administrada y mantenida por una sola entidad dentro de una sola organización, tiene un uso limitado.

Las redes blockchain se vuelven más valiosas cuando más organizaciones participan para compartir y realizar transacciones de datos. Pero estas organizaciones solo pueden participar cuando se les ha concedido permiso. Este tipo de red autorizada, entre un conjunto conocido de participantes, es el tipo de blockchain al que se refiere a blockchains privados.

2. *Consensos*

Las transacciones en cadenas de bloques públicas y privadas se verifican por consenso, pero hay muchas formas diferentes en las que se puede lograr el consenso.

Incluso dentro del espacio blockchain sin permiso, los mecanismos de consenso pueden variar ampliamente. Pero, en general, se basan en una estructura de incentivos que recompensa a los participantes que contribuyen a la red. El mecanismo que probablemente sea el más conocido, gracias a **Bitcoin** y otras criptomonedas, es una prueba de funcionamiento.

Los mineros participan en la red aportando su poder de cómputo para resolver problemas criptográficos complejos para verificar transacciones, y son recompensados en forma de criptomoneda. La prueba de trabajo es un mecanismo de consenso computacionalmente intensivo y que requiere mucho tiempo, lo que resulta en velocidades de transacción lentas y altos costos de electricidad.

Por esta razón, han surgido muchos otros mecanismos de consenso en el espacio público de la cadena de bloques, como la prueba de participación, la prueba de capacidad y la prueba del tiempo transcurrido.En una cadena de bloques privada, el consenso generalmente se logra a través de un proceso llamado respaldo selectivo. Se basa en el concepto de que los participantes de la red han obtenido permiso para estar allí y que los participantes involucrados en una transacción pueden confirmarlo.

La ventaja es que una cadena de bloques que utiliza este tipo de consenso se puede construir con una arquitectura más modular y puede permitir un mayor volumen de transacciones a velocidades más rápidas. Los patrocinadores están determinados por las reglas de gobierno y operación de la red.

3. *Security*

La seguridad ofrecida en una cadena de bloques pública depende del mecanismo para registrar transacciones. Anteriormente, mencioné el concepto de inmutabilidad, pero probablemente sea más exacto decir que las cadenas de bloques son evidentes. Una vez que una transacción se registra en la cadena de bloques, no se puede alterar ni encubrir, solo se puede revertir con una nueva transacción. Tanto la transacción original como la posterior aún son visibles. Los grupos de transacciones se agrupan en un bloque que está protegido criptográficamente y vinculado al bloque anterior. Esto crea una cadena y una cadena es mucho más difícil de piratear que un solo eslabón.

Sin embargo, si una mayoría malintencionada de la red se coludiera, podría potencialmente obtener el control del proceso de aprobación de la transacción. Esto se conoce como un ataque del 51 por ciento.

Las cadenas de bloques privadas también emplean el mecanismo de grabación de agrupar transacciones en bloques y vincular bloques en una cadena inmutable. Pero en un contexto empresarial, cuando es necesario proteger la información corporativa confidencial y los datos de los clientes, es importante proteger la cadena de bloques con medidas adicionales. Su red blockchain debe estar preparada para:

- Asegurar la separación entre entidades, brindando protección horizontal.
- Evite ataques a través de cuentas de usuario privilegiadas, proporcionando protección vertical.
- Proteja los datos cifrados asegurando las claves criptográficas.

4. *Rendimiento*

Las cadenas de bloques públicas tienden a tener un rendimiento de transacción más bajo que las cadenas de bloques privadas debido al tiempo y al cálculo requerido para confirmar las transacciones. Hasta que se complete la prueba de trabajo para la transacción actual, las transacciones posteriores se retrasan.

El rendimiento de una cadena de bloques privada depende del diseño de la red y su infraestructura de sistemas. Dado que el respaldo selectivo no requiere ni cerca de la cantidad de energía que requiere la prueba de trabajo, una cadena de bloques privada puede procesar volúmenes de transacciones mucho más altos a velocidades más altas con muchos menos recursos computacionales.

En última instancia, si el consenso está automatizado y tiene un sistema de entrada y salida escalable con mucha memoria, un caché grande y un microprocesador comercial rápido, debería ser capaz de entregar y procesar grandes volúmenes de datos en su cadena de bloques privada.

5. *Escalabilidad*

El rendimiento y la escalabilidad a menudo van de la mano. Debido a la potencia computacional requerida para ejecutar cadenas de bloques públicas y garantizar el consenso, pueden ser difíciles de mantener a gran escala. Cuantos más usuarios se unan a una red pública, más transacciones solicitan, más tardan en confirmarse esas transacciones y mayores son los tiempos de espera durante las horas pico. La mayoría de las cadenas de bloques privadas comienzan con poco, pero necesitan espacio para crecer para manejar la cantidad de socios internos y externos que participarán en la red.

Puede ser difícil ahora determinar sus requisitos futuros o predecir cómo crecerá su red, por lo que es importante tener una arquitectura modular, capacidades de escalamiento horizontal y capacidad bajo demanda.

3) Cómo funciona un blockchain

Cabe destacar que el uso de bloques dentro de una red tiene una mayor complejidad al momento de describir cómo es que funciona sobre todo al abordar temas como la seguridad y la distribución de los datos, sin embargo, de manera general podemos decir que el proceso de compartir bloques es elsiguiente.

1. *A medida que ocurre cada transacción, se registra como un "bloque" de datos*

Esas transacciones muestran el movimiento de un activo que puede ser tangible (un producto) o intangible (intelectual). El bloque de datos puede registrar la información de su elección: quién, qué, cuándo, dónde, cuánto e incluso la condición, como la temperatura de un envío de alimentos.

2. *Cada bloque está conectado a los anteriores y posteriores.*

Estos bloques forman una cadena de datos a medida que un activo se mueve de un lugar a otro o la propiedad cambia de manos. Los bloques confirman la hora exacta y la secuencia de las transacciones, y los bloques se enlazan de forma segura para evitar que se altere cualquier bloque o que se inserte un bloque entre dos bloques existentes.

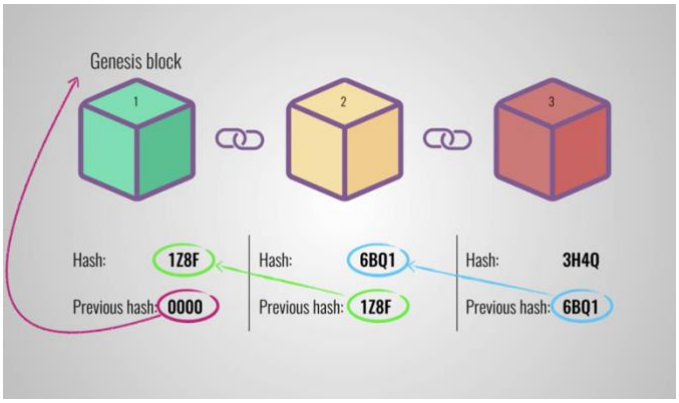

Imagen 3: Diagrama de comunicación y de ligado entre bloques a través de llaves hash.

3. *Las transacciones se bloquean juntas en una cadena irreversible: una cadena de bloques*

Cada bloque adicional refuerza la verificación del bloque anterior y, por lo tanto, toda la cadena de bloques. Esto hace que la cadena de bloques sea evidente, brindando la fuerza clave de la inmutabilidad. Esto elimina la posibilidad de manipulación por parte de un actor malintencionado y crea un registro de transacciones en las que usted y otros miembros de la red pueden confiar.

4) Beneficios del blockchain

1. *Mayor confianza*

Con blockchain, como miembro de una red exclusiva para miembros, puede estar seguro de que está recibiendo datos precisos y oportunos, y de que sus registros confidenciales de blockchain se compartirán solo con los miembros de la red a los que haya otorgado acceso específicamente.

2. *Mayor seguridad*

Se requiere un consenso sobre la precisión de los datos de todos los miembros de la red, y todas las transacciones validadas son inmutables porque se registran permanentemente. Nadie, ni siquiera un administrador del sistema, puede eliminar una transacción.

3. *Más eficiencias*

Con un libro mayor distribuido que se comparte entre los miembros de una red, se eliminan las conciliaciones de registros que hacen perder tiempo. Y para acelerar las transacciones, un conjunto de reglas, llamado contrato inteligente, puede almacenarse en la cadena de bloques y ejecutarse automáticamente.

B. Contratos Inteligentes

Con base a lo que previamente conocemos de Blockchain, podemos entender que un smart contract es un tipo especial de instrucciones que es almacenada en la blockchain. Y que además tiene la capacidad de autoejecutar acciones de acuerdo a una serie de parámetros ya programados. Todo esto de forma inmutable, transparente y completamente segura.

Sin embargo, antes de entender como funciona un smart contract o contrato inteligente debemos entender como tal qué es un contrato:

"Un contrato no es más que un acuerdo entre dos o más partes, un entorno donde se define lo que se puede hacer, cómo se puede hacer, qué pasa si algo no se hace."

Es decir, unas reglas de juego que permiten a todas las partes que lo aceptan entender en qué va a consistir la interacción que van a realizar.

Sin embargo, hasta antes de la llegada del bitcoin los contratos han sido documentos verbales o caros documentos escritos. Estos documentos están sujetos a las leyes y jurisdicciones territoriales, y en ocasiones requieren de notarios, incluso lo peor es que los contenidos de estos pueden estar sujetos a la interpretación.

Es aquí donde precisamente en el 2009 llegan los denominados smart contract, un contrato inteligente es capaz de ejecutarse y hacerse cumplir por sí mismo, de manera autónoma y automática, sin intermediarios ni mediadores. Evitan el lastre de la interpretación al no ser verbal o escrito en los lenguajes que hablamos. Los smart contracts se tratan de "scripts" (códigos informáticos) escritos con lenguajes de programación. Esto quiere decir que los términos del contrato son puras sentencias y comandos en el código que lo forma.

Es importante destacar que, al estar distribuido por miles de ordenadores, se evita que una gran compañía los custodie, lo que elimina burocracia, censuras y los grandes costes / tiempos implícitos de este proceso que, dicho sea de paso, hasta ahora es el custodio.

Si juntamos los principios de un smart contract con la creatividad de muchos desarrolladores del planeta, el resultado son posibilidades jamás vistas, accesibles para todos y a costes que rozan la gratuidad. Ecosistemas sin figuras autoritarias que someten a su voluntad a sus integrantes. Hablamos de un mundo más justo. Imagina un coche Tesla autoconducido, comprado en grupo, capaz de autogestionarse y alquilarse por sí solo. Todo ello sin una compañía tipo Uber detrás llevándose el 10 %. De esa podemos decir: bienvenido al mundo de los contratos inteligentes.

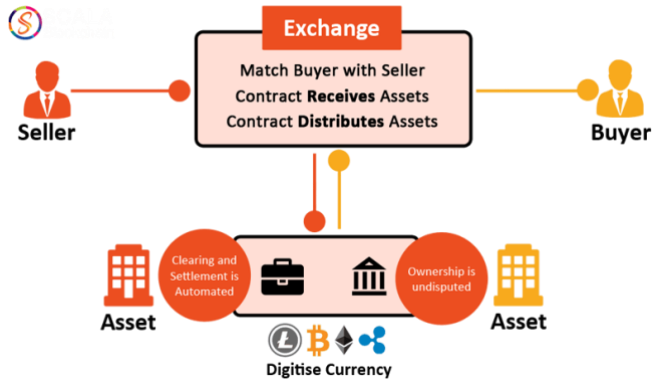

Imagen 4: Generalización del uso de contratos inteligentes dentro de cadenas de bloques para realizar transacciones mediante criptomonedas

1) Contrato inteligente en bitcoin

Los contratos inteligentes son útiles en una amplia variedad de dominios. Para explicar cómo funciona un contrato inteligente, considere el siguiente escenario de la vida real.

Un claro ejemplo es el pensar en subarrendar un condominio de su propiedad en un futuro cercano. Con contratos inteligentes en la Blockchain de Bitcoin (BSV), su inquilino puede pagar el alquiler con Bitcoin. Los contratos inteligentes administrarán el proceso de liquidación automáticamente, notificando a su inquilino cuando vence el alquiler en una fecha predefinida, reduciendo así la carga para el propietario.

Una vez que se ha enviado el pago, el contrato inteligente valida la recepción del pago. El acuerdo digital emite recibos y registra la transacción en el libro mayor de Bitcoin (BSV).

Se puede programar un contrato inteligente de modo que solo después de que expire el contrato de arrendamiento y se realicen todos los pagos, el depósito inicial en garantía se devolverá a la cuenta del inquilino.

Otro ejemplo es que dos partes están involucradas en un grupo de deportes de fantasía o en apuestas. El contrato inteligente puede pagar automáticamente al ganador una vez que se haya decidido el concurso para reducir el riesgo de fraude. Los costos se reducen y no hay necesidad de participación de terceros.

C. Criptomonedas

Una criptomoneda es una moneda digital creado en base a un código. Dicha criptomoneda se puede emplear como un medio de pago electrónico, es un sustituto de dinero que no está controlada por ningún ente gubernamental ni privado. Su fuerza está respaldada por medio de la confianza que los usuarios tengan en ella. En otras palabras, su precio está basado en la oferta y demanda de esta.

Se pueden dar muchas definiciones de criptomoneda. Según el Banco Central Europeo "es la representación digital de valor, no emitida por ninguna autoridad central, institución de crédito o emisor de dinero electrónico reconocido que en ciertas ocasiones, puede ser utilizada como medio de pago alternativo al dinero".

También podríamos definirlas como un sistema de pago a través de Internet, basadas en un sistema peer-to-peer o red entre iguales (P2P), que contienen un elemento de seguridad basado en la criptografía y en donde el valor es transmitido electrónicamente entre las partes, sin un intermediario.

1) Aspectos tecnológicos

Las criptomonedas se emiten al margen de los gobiernos y bancos centrales y, al menos en teoría, esta función se traslada a todo aquel que quiera participar. Esta generación de moneda se denomina "minado". Estos participantes (mineros) son quienes aportan la seguridad a las transacciones utilizando, en la mayor parte de los casos, la tecnología de blockchain (cadena de bloques).

Blockchain es un gigantesco libro de contabilidad distribuido en el que los registros (bloques) están enlazados para proteger la seguridad y la privacidad de las transacciones. Se trata de una base de datos distribuida y segura gracias a la utilización de algoritmos criptográficos.

Al realizar una transacción hay varios usuarios (nodos) que se encargan de verificar la transacción y registrarlas en el gigantesco libro de cuentas. Veamos el funcionamiento con un ejemplo. Imaginemos que A quiere enviar a B una determinada cantidad X. Si esta transacción se realizara mediante una transferencia bancaria, A le pediría a su banco que retirara X de su cuenta para enviarla a la cuenta de B. Lo restarían de su saldo, comunicando al otro banco que debe añadir X a la cuenta de B.

Pues bien, esta misma transacción realizada con criptomonedas, tal y como se representa en el en el siguiente gráfico elaborado específicamente para este trabajo, funcionaría de esta forma. La primera diferencia sustancial es que nadie sabrá quién es A ni B, únicamente que desde un monedero digital (equivalente a la cuenta bancaria) se quiere transferir una cantidad a otro monedero.

A envía un mensaje a los usuarios notificando su intención. Estos comprueban que tiene saldo suficiente. Si es así, anotan esta transacción de forma provisional. Conforme pasa el tiempo y se van completando más transacciones se va conformando un bloque. Al llegar a la capacidad de la cadena de bloques se procede a validarlo.

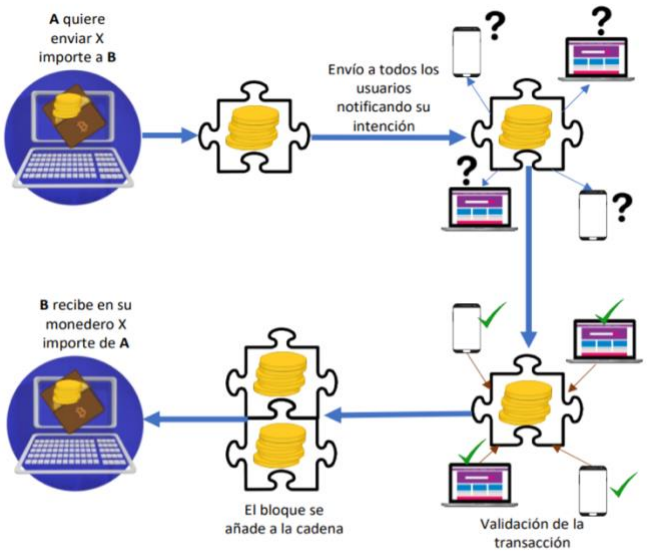

Imagen 5: Sistema blockchain aplicado en la moneda criptográfica "Bitcoin".

Mediante complicados algoritmos matemáticos que requieren elevada potencia de computación, y por lo tanto alto consumo energético, los bloques quedan registrados de forma permanente en la cadena.

Uno solo de estos bloques no podría ser modificado sin alterar todos los que están enlazados con él, algo que sería realmente improbable pues el resto de los nodos lo deberían validar. Este mecanismo asegura la integridad de la operación.

En el proceso de minado, los mineros reciben avisos de nuevas transacciones agrupadas A quiere enviar X importe a B, B recibe en su monedero X importe de A Envío a todos los usuarios notificando su intención Validación de la transacción

El bloque se añade a la cadena en bloques. Unos compiten con otros y el primero que consigue crear un bloque válido recibe una recompensa por el servicio, en la criptomoneda que esté operando.

La cadena de bloques está sincronizada entre los nodos de forma irreversible. Nadie podrá modificar el libro de registro sin que el resto se entere. Esta tecnología permite asimismo asegurar la trazabilidad de las transacciones. Aunque no sean conocidas las identidades de A y B, es público el camino que ha seguido el envío. La transferencia de A a B se realiza de forma rápida y sin comisiones.

2) Minería

Es uno de los términos relacionados con las criptomonedas que más vamos a escuchar. La razón se debe, a que la minería es un proceso fundamental para las criptomonedas.

Es básicamente el proceso por el cual se crean las criptomonedas. Cada nueva criptomoneda que es generada en la red se hace gracias al minado de esta. Ahora el término parece bastante apropiado, ¿no? Aunque la minería es mucho más que eso, también se encarga de confirmar las transacciones que se realizan en la Blockchain (un término que veremos a continuación).

Los llamados mineros, que son las personas encargadas de confirmar las transacciones, de manera segura y descentralizada, emplean una red p2p o peer-to-peer, una red par a par, para llevar todo esto a cabo. A esas personas reciben una comisión en criptos por completar cada operación.

La Blockchain o Cadena de Bloques, se puede definir como una especie de base de datos pública, transparente, a la cual todo el mundo puede tener acceso solo para visualizar los datos. A través de las cadenas de bloques se realizan todas las transacciones relacionadas con criptomonedas.

Una de sus características principales es que sus registros son permanentes, una vez que algo queda guardado en la Blockchain, no puede eliminarse. Y es sostenida por todos los equipos que participan en la minería, completando y confirmando todas las transacciones.

3) Regulación de las criptomonedas

En el ámbito de las criptomonedas la falta de regulación llega al extremo de no existir ni siquiera un consenso internacional en su definición. En algunos países son consideradas mercancías (en Canadá para efectos fiscales), en otros fondos transferibles, activos financieros, etc.

La realidad actual es que el tratamiento de las criptomonedas no sólo varia de un país a otro sino que dentro del mismo país tiene distintos enfoques según se analicen desde el punto de vista financiero, legal, cambiario o tributario.

El hecho de anunciar su posible regulación desencadena una bajada en su valor. En los primeros días de enero de 2018 el precio del bitcoin bajó un 14% en una sola jornada al anunciar el gobierno que está trabajando en un proyecto de ley para prohibir las transacciones con criptomonedas.

	Advertencias al consumidor	Reglas sobre Blanqueo y financiación terrorismo	Tratamiento tributario	Registro/licencias intermediarios	Proyectos internacionales blockchain
España	X	X	X	X	X
EEUU	X	X	X	X	X
Canadá		X	X	X	X
Brasil	X		X		X
Japón		X	X	X	X
Unión Europea	X	X	X	X	X
Alemania	X		X		X
Suiza		X	X	X	
Francia	X			X	X
Reino Unido	X		X	X	X
Singapur	X	X	X	X	X
Filipinas		X		X	
Chile					X
Colombia	X				

Imagen 6: La siguiente table muestra la situación regulatoria de algunos países

4) Regulación en México de activos virtuales

La Ley para Regular las Instituciones de Tecnología Financiera propone considerar el uso de activos virtuales, con previa autorización del Banco de México. Se dedica el Artículo 30 su definición: “Se considera activo virtual la representación de valor registrada electrónicamente y utilizada entre el público como medio de pago para todo tipo de actos jurídicos y cuya transferencia únicamente puede llevarse a cabo a través de medios electrónicos.”

El Banco de México tiene la facultad de definir qué criptomonedas contarán con su autorización para ser utilizadas legalmente en México y bajo qué restricciones se podrán utilizar.

No son monedas de curso legal en México, ya que el Banco de México no los emite ni respalda. De igual manera, tampoco son divisas extranjeras porque ninguna autoridad monetaria extranjera los emite ni respalda.

DINERO AUTORIZADO	CRIPTOMONEDAS
Billetes y monedas físicos	Monedas virtuales
Los billetes y las monedas físicas son de curso legal	Las monedas virtuales de las criptomonedas no son curso lega
Respaldados por las regulaciones del gobierno y por las leyes	Gobernadas por protocolos públicos de operación y por un algoritmo
El valor afectado por la economía del gobierno que emite	El valor es afectado por la confianza general en la moneda y en el algoritmo
La creación y distribución de billetes y monedas son determinados por los bancos centrales	El número de las monedas es determinados por los protocolos de la moneda
Los bancos y otras instituciones financieras tienen moneda a nombre de los depositantes y mantienen un registro de esos depósitos	La propiedad de la moneda está registrada en un libro mayor público distribuido
La transferencia electrónica de la moneda es administrada principalmente por los banco	Transferencias par-a-par, administradas por una red que las registra en el libro mayor público

Imagen 7: La siguiente tabla muestra las diferencias que existe entre el dinero físico y las criptomonedas

5) Principales criptomonedas

El **Bitcoin** es sin duda la criptomoneda más popular y extendida en el mundo. En 2008SatoshiNakamoto8 publicó en 2008 un artículo9 en el que anunciaba que había desarrollado un nuevo sistema de pago electrónico, estando, basado en el trabajo que, sobre la base de la criptografía de clave pública que daba una solución al problema de los pagos electrónicos había publicado WeiDai describiendo lo que denominó el bMoney.

En 2009 se publicó en el portal P2P, nuevamente bajo el nombre de SatoshiNakamoto, un mensaje de este en el que presentaba el portal oficial de bitcoin, las características fundamentales de esta nueva moneda digital describieron el protocolo bitcóin, pero no fue hasta 2009 cuando la divisa entró en funcionamiento.

El segundo lugar en capitalización lo ocupa **Ethereum**. En realidad, la moneda se llama mether y Ethereum hace referencia a un sistema que permite a los usuarios crear aplicaciones basadas en monedas virtuales que pueden ir más allá de su simple uso financiero al sistema que la controla.

Lo más destacado de esta criptomoneda es su elevada velocidad de transacción y también que ha introducido en el mundo virtual el concepto de contratos inteligentes. Este método permite a usuarios o empresas firmar contratos sin comisiones ni control por parte de ningún país.

Litecoin es una criptomoneda que permite realizar pagos instantáneos y de costo casi cero a cualquier parte del mundo. La ventaja de Litecoin es que provee tiempos de confirmación de transacción más rápidos que cualquier otra. Es una red súper simple para aquellos que necesitan mover pequeñas cantidades de dinero rápidamente.

La relevancia de bitcoin en el mundo de las criptomonedas es innegable, hasta el punto de que existe una denominación concreta para referirse a las criptomonedas diferentes al bitcoin o que se han creado como una alternativa al protocolo original. Son las Altcoins. Se pueden diferenciar dos grupos.

El primero incluye las criptomonedas que provienen de una bifurcación (fork) de bitcoin, como son Litecon, Dogecoin, entre otras; y un segundo grupo que han construido su propio blockchain, utilizando hasta algoritmos de minería diferentes al de bitcoin. En este grupo encontramos a Ethereum, Nxt.

Imagen 8: Algunas criptomonedas que existe en el mercado aunque las más conocidas son bitcoin (BTC) y el ether(ETH)

6) Bitcoin en el futuro

Los precios de Bitcoin y criptomonedas se han disparado esta semana, con el valor combinado del mercado de criptografía de nuevo acercándose a $2 billones.

El precio del bitcoin, después de comenzar el año en torno a los 30.000 dólares por bitcoin, se ha duplicado, subiendo debido a la adopción institucional de Wall Street y el interés corporativo del multimillonario de Tesla Elon Musk (y más compradores podrían estar en camino).

Ahora, la analista de Deutsche Bank y economista de Harvard Marion Laboure ha pronosticado que 'los próximos dos o tres años deberían ser un punto de inflexión para el bitcoin', señalando la trayectoria de Tesla como una posible hoja de ruta para que bitcoin 'transforme el potencial en resultados'.

Sin embargo, Laboure espera que el precio del bitcoin 'siga siendo ultravoltil' y advierte que 'algunas compras grandes adicionales o salidas del mercado podrían afectar significativamente el equilibrio entre la oferta y la demanda'.

La compañía de coches eléctricos Tesla de Elon Musk impactó este equilibrio el mes pasado cuando reveló que había comprado bitcoin por valor de 1.500 millones de dólares, enviando el precio del bitcoin fuertemente más alto. Sin embargo, los laboristas ve una conexión más profunda entre la pareja.

Tanto Tesla como bitcoin han seguido una trayectoria similar en el último año y, según Labore, el sentimiento del

mercado hacia Tesla 'comenzó a cambiar significativamente en los últimos 18 meses a medida que Tesla dio los primeros resultados'.

"Tesla es cinco años mayor que el bitcoin y siempre ha desatado sólidos debates entre las personas que lo ven como una moda que pronto morirá y aquellos que lo ven como el futuro del coche" – Laboure

Este analista ha argumentado que un consenso sobre el futuro del bitcoin puede surgir a medida que la gente monitorea la evolución de la moneda digital en los próximos dos o tres años.

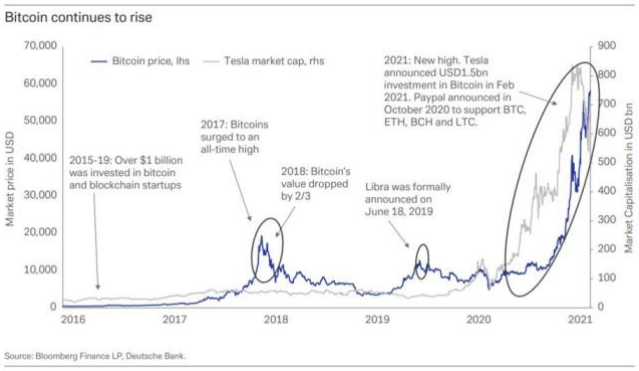

Imagen 9: Precio del bitcoin en el mercado desde 2016 hasta inicios del 2021

Mientras tanto, la reciente adopción en Wall Street (incluyendo Morgan Stanley MS -1.2% preparándose para ofrecer a los clientes ricos la capacidad de invertir en fondos bitcoin y JPMorgan mirando opciones de cámaras de compensación criptográficas) ha empujado firmemente bitcoin en el radar de la industria financiera tradicional.

Imagen 10: El bitcoin hoy en día es la criptomoneda más famosa y de mayor interacción dentro del mercado.

'Érase una vez, los corredores establecidos y los bancos cancelaron el cripto como 'demasiado volátil', negándose a reconocerlo como una clase de activos legítimos en el asesoramiento emitido a los inversores', dijo Stephen Kelso, jefe de mercados de capitales de ITI Capital.

Sin embargo, también vemos que hay un cambio dramático en el enfoque de las organizaciones institucionales, que ven cada vez más la inversión criptográfica como una tienda de valor relevante contra la rápida aceleración de la degradación de las monedas fiduciarias.

III. Relación con los Sistemas Distribuidos

Una de las características principales del blockchain, las criptomonedas y los contratos inteligentes son el uso de redes Peer to Peer o P2P que en español se les conoce como red entre pares o red de igual a igual. Son un tipo de redes descentralizadas. Redes que están formadas por cientos e incluso millones de ordenadores ubicados en todo el mundo. Todas ellas funcionando bajo un mismo protocolo de comunicaciones, con el objetivo de crear una enorme red para compartir información de cualquier índole.

Es decir, es una red donde no hay un punto central de conexión o control, y donde las partes actúan de forma autónoma respondiendo a un protocolo de comunicaciones y consenso común. De esta forma, los integrantes de la red pueden intercambiar información de forma directa y sin intermediarios.

1) Tipos de redes P2P

Entre los tipos de redes P2P existentes podemos especificar los siguientes:

Red descentralizada y estructurada son conocidas como redes P2P híbridas. En este tipo de redes no existe un directorio en un servidor central, sino que en su lugar existen una serie de nodos o peers, que tienen la capacidad de recibir peticiones de información y responder a las mismas para facilitar el acceso a los recursos. Para evitar la centralización de esta funcionalidad, los nodos o peer especiales pueden ser instalados y configurados por cualquier persona, buscando con ello que la misma comunidad de usuarios extienda la funcionalidad de la red y permita su correcto funcionamiento.

Otro tipo sería el caso de las ***Redes descentralizadas y no estructuradas***, en este tipo de redes P2P no existen ordenadores o nodos que funcionen como

controladores centrales de peticiones. Por el contrario, cada nodo dentro de la red tiene las mismas funciones que el resto de nodos, por lo que cada nuevo nodo ejerce la misma autoridad que el resto. En este punto, redes como Bitcoin cumplen con esta características, puesto que cada nodo conectado tiene las mismas capacidades que el resto.

2) Directorios Descentralizados

Un problema complejo, pero la situación se puede solventar de una forma bastante efectiva con dos medidas bien definidas:

- En primer lugar, hacer que el software sea capaz de compartir información de conexión sobre quienes ejecutan el mismo. Así, cada computador que ejecuta el software es capaz de tener un directorio de computadores conectados y servirse de ellos para conectarse al nodo que desea.

- Incentivar la mayor descentralización posible de la red. Es decir, hacer que muchas personas ejecuten el software creando sus propios nodos, y por tanto aumentando el tamaño de la red. De esta manera, se mejora su alcance y las posibilidades de la misma.

Es decir, mientras más pares o peers (computadores ejecutando el software P2P) tenga la red, más posibilidades hay de que la red no pueda ser censurada, su funcionamiento será más resistente y, mejores capacidades tendrá la misma.

3) Ventajas y desventajas

En el caso de las ventajas de este tipo de tecnologías serían:

- Una red P2P es resistente a la censura. Una red P2P altamente descentralizada es prácticamente imposible de censurar.

- Ofrecen un resiliencia inigualable. Si un nodo cae, otro nodo puede tomar su lugar. Por eso dicen que las redes P2P pueden sobrevivir a una catástrofe nuclear, porque estas pueden destruir muchos nodos, pero si solo uno sobrevive, la red puede reconstruirse por completo.

- Las redes P2P pueden llevar a soluciones de escalabilidad potentes para presentar servicios únicos con alcance global.

- Al no depender de entidades centrales, las P2P generan más confianza en sus usuarios.

- Ofrecen un alto nivel de ancho de banda. Esto gracias a que aprovechan el ancho de banda de cada participantes, para transformarlo en propio de la red.

- Sirven para transmitir información digital de cualquier tipo. Desde tu canción favorita a cientos de millones de dólares, en segundos.

Como cualquier software o tecnología siempre existirán desventajas que s presenten al comparar con su competencia, en el caso concreto de las redes P2P, sus desventajas son:

- Una red P2P es resistente a la censura, pero no te hace anónimo a menos que esté diseñada para ello, incluso, si esa red usa cifrado. El mejor ejemplo es BitTorrent, donde los ISP pueden detectar el uso del protocolo, y con ello advertir a las autoridades de la descarga ilegal por parte de un usuario.

- El diseño de las redes P2P generan que a mayor tamaño aumente la latencia. Es decir, para que una información llegue a todas las partes que forma la red, se tomará más tiempo en una red P2P de gran tamaño que en una de menor tamaño. De allí que se busquen nuevos algoritmos y protocolos que ayuden a superar este problema.

- Los protocolos P2P tienen una serie de problemas estructurales conocidos. Casos como los ataques MITM para tomar el control de nodos, debido a que estos deben estar conectados todo el tiempo de forma pública son uno de estos fallos. También los protocolos son susceptibles a ataques de enrutamiento o cosas tan sigilosas como un ataque Eclipse o un ataque Erebus.

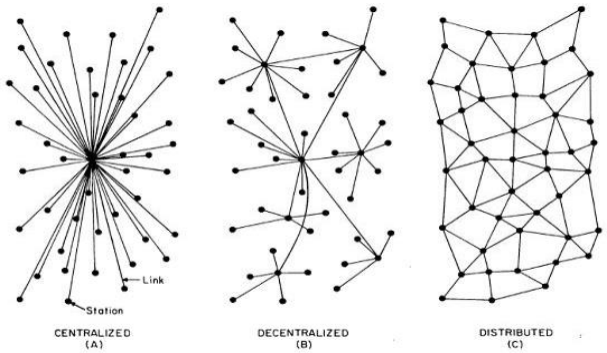

Imagen 11: Redes de distribución de datos

IV. Conclusión

Desde la liberación del diseño y código de Bitcoin, en 2009, tecnologías como el Blockchain y el Smart Conctract han experimentado un continuo avance y cambio, especialmente en el contexto de la concepción de nuevas aplicaciones de los sistemas descentralizadas y sobre todo de los sistemas distribuidos.

Si bien el origen de la tecnología está en la creación de criptomonedas como Bitcoin o las alt-coins que le siguieron, lan realidad es que actualmente el blockchain ya no se limita a ese uso, sino que se han extendido a prácticamente cualquier área en la que se pueda repensar la interacción para hacerla descentralizada, al modo de los sistemas P2P.

Por otro lado, si bien la programación y visualización de los Smart Contracts para las transacciones dentro del blockchain o dentro de las criptomonedas requiere una especialización y comprensión de la tecnología bastante profunda, es importante sobre todo conocer y saber como funcionan en este contexto para de manera general tener en cuenta que la seguridad no solamente se da alrededor de la misma cadena de bloques.

V. Referencias

[1] "What is Blockchain Technology? - IBM Blockchain", *Ibm.com*, 2021. [Online]. Available: https://www.ibm.com/blockchain/what-is-blockchain?cm_mmc=OSocial_Youtube-_-Blockchain+and+Watson+Financial+Services_Blockchain-_-WW_WW-_-YTDescription-101-Blockchain-Explained-LP-What-is-Blockchain&cm_mmca1=000026VG&cm_mmca2=10007330. [Accessed: 21- Mar- 2021]

[2] T. Laurence, *Blockchain For Dummies*, 2nd ed. 2020.

[3] K. Wüst and A. Gervais, "Do you Need a Blockchain?," *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, Zug, Switzerland, 2018, pp. 45-54, doi: 10.1109/CVCBT.2018.00011.

[4] J. M. Montes, C. E. Ramirez, M. C. Gutierrez and V. M. Larios, "Smart Contracts for supply chain applicable to Smart Cities daily operations," *2019 IEEE International Smart Cities Conference (ISC2)*, Casablanca, Morocco, 2019, pp. 565-570, doi: 10.1109/ISC246665.2019.9071650.

[5] "CRIPTOMONEDAS", *Pj.gov.py*, 2021. [Online]. Available: https://www.pj.gov.py/ebook/monografias/extranjero/civil/Julia-Sanchez-Criptomonedas.pdf. [Accessed: 22- Mar- 2021]

[6] "¿Qué es Bitcoin? ¿Cómo funciona? ¿Dónde se compran? ", *Computerhoy.com*, 2021. [Online]. Available: https://computerhoy.com/. [Accessed: 22- Mar- 2021]

[7] Criptomonedas ¿el dinero del futuro ?", *Computerhoy.com*, 2021. [Online]. Available: http://ciencia.unam.mx/leer/822/criptomonedas-el-dinero-del-futuro/. [Accessed: 22- Mar- 2021]

[8] B. Bambrough, "Bitcoin Price Prediction: Tesla 'Reveals' Potential Future For Bitcoin", *Forbes*, 2021. [Online]. Available: https://www.forbes.com/sites/billybambrough/2021/03/18/as-bitcoin-and-crypto-near-2-trillion-deutsche-bank-has-made-a-surprise-bitcoin-price-prediction/?sh=63b4465618fe. [Accessed: 22- Mar- 2021]