Capítulo 1 - Blockchain

Narcisa Medranda Morales
Miguel Arcos Argudo

SciELO Books / SciELO Livros / SciELO Libros

MEDRANDA MORALES, N., and ARCOS AGUDO, M. Blockchain. In: *Blockchain, criptoactivos y metaverso*. Una aproximación teórica [online]. Quito: Editorial Abya-Yala, 2023, pp. 13-40. ISBN: 978-997-810-802-4. Available from: https://books.scielo.org/id/pb8tf. https://doi.org/10.17163/abyaups.6

All the contents of this work, except where otherwise noted, is licensed under a Creative Commons Attribution 4.0 International license.

Todo o conteúdo deste trabalho, exceto quando houver ressalva, é publicado sob a licença Creative Commons Atribição 4.0.

Todo el contenido de esta obra, excepto donde se indique lo contrario, está bajo licencia de la licencia Creative Commons Reconocimento 4.0.

Capítulo 1

Blockchain

Origen de la *blockchain*

Si bien es cierto que el auge de la moneda digital *bitcoin* ha dado a conocer la tecnología de la cadena de bloques (*blockchain*), también lo es que las bases en las cuales se sustenta se remontan a 1991, cuando los científicos Stuart Haber y W. Scott Stornetta introdujeron la idea de una propuesta teórica con la finalidad de proporcionar una solución computacional para documentos digitales con marca en el tiempo. En este trabajo plantearon una cadena concreta de bloques protegidos mediante un criptograma.

Una *blockchain* puede ser entendida como una secuencia de paquetes de datos llamados bloques, enlazados unos a otros mediante un código criptográfico único, que contienen información en formato digital, la cual se almacena en una red colaborativa de ordenadores operada por una comunidad de personas a los que se les denomina "mineros". La principal característica de esta red radica en que todos sus nodos tienen almacenada la misma información, constituyendo una base de datos distribuida.

En 2008, Satoshi Nakamoto[1] publica el artículo *Bitcoin: A Peer-to-Peer Electronic Cash System*, en el cual se explica el funcionamiento de una versión "*peer- to-peer*" (por pares) de dinero virtual que no requiere de intermediarios ni terceras partes para realizar su registro, haciendo posible los pagos en línea (*on-line*) sin la participación de una entidad (como los bancos) u organismo central. Además, se detalla la tecnología de cadena de bloques (*blockchain*) cuya función era poner en práctica

1 Pseudónimo utilizado por la persona o las personas creadoras del *bitcoin*.

un sistema de registro de todas las transacciones de que se realizarán con estos *bitcoins,* otorgándole confiabilidad y seguridad ante la imposibilidad de falsificar las identidades y las transacciones, basados en el sistema criptográfico (Huillet, 2019). De esta manera, en enero de 2009 se realiza la primera transacción con *bitcoin*.

Para 2013, Vitalik Buterin empieza el desarrollo de una nueva plataforma de computación distribuida basada en *blockchain*, por considerar que el *bitcoin* requería un lenguaje para la creación de aplicaciones descentralizadas. Finalmente, creó su propio proyecto, dando origen a los contratos inteligentes y a *Ethereum*, la segunda moneda digital con mayor popularidad en la actualidad (Binance Academy, 2018a).

Glosario sobre *blockchain*

En esta sección se incluyen algunos conceptos básicos relacionados con la *blockchain* y las criptomonedas (basados en Vigna y Casey, 2016, citados por Arrasco, 2021), con la finalidad de facilitar la comprensión de los distintos aspectos a tratar y en los cuales se profundiza a lo largo de este trabajo.

- Base de datos centralizada: estructura de almacenamiento de datos centralizado en un solo ordenador.
- Base de datos distribuida: estructura de almacenamiento de datos almacenados en distintos ordenadores ubicados físicamente en distintos lugares geográficos.
- Bloque de recompensa (*block reward*): se refiere a la recompensa que se otorga a un minero después de haber realizado un *hash* de un bloque de transacción. Pueden ser una combinación de monedas y tarifas de transacción, dependiendo de la política utilizada por la criptomoneda en cuestión y si todas las monedas ya se han extraído con éxito.
- *Bounty*: una recompensa que se paga por completar una tarea determinada. Las tareas incluyen identificar vulnerabilidades de

código, crear contenido, trabajo de diseño, investigación, traducciones, impacto social y más.

- Cadena de bloques (*blockchain*): un libro mayor digital consensuado compuesto por datos inmutables y grabados digitalmente en paquetes llamados bloques. Cada bloque está unido al siguiente mediante una firma criptográfica, permitiendo que las cadenas de bloques actúen como un libro mayor, con la posibilidad de ser compartido y es accesible a cualquier persona con los permisos adecuados.
- Clave privada (*private key*): es una cadena alfanumérica de datos que corresponde a una sola cartera específica. Pueden considerarse como una contraseña que permite a una persona acceder a su cartera.
- Clave pública (*public key*): clave que puede ser utilizada por cualquier persona. Se utiliza para cifrar mensajes que se quieren enviar a un destinatario, quien podrá descifrarlo teniendo conocimiento de qué tipo de clave pública se trata y de su propia clave privada (*private key*).
- Contratos Inteligentes (*smart contracts*): son programas cuyos términos se registran en un lenguaje informático, en lugar de lenguaje legal. Son acciones automatizadas que se pueden codificar y ejecutar una vez que se cumple un conjunto de condiciones.
- Criptomoneda: moneda digital que se basa en las matemáticas y utiliza técnicas de encriptación para regular la creación de unidades monetarias, así como verificar la transferencia de fondos. Estas operan independientemente de un banco central.
- Dirección de cartera (*adress wallet*): se utiliza para enviar y recibir transacciones en una red *blockchain*. Una dirección es una cadena de caracteres alfanuméricos, que también se puede representar como un código QR escaneable.
- Firma digital (*digital signature*): código generado por cifrado de clave pública y adjunto a un documento transmitido electrónicamente para verificar el contenido del documento.
- Huella digital (*hash*): función que toma una entrada y, luego, genera una cadena alfanumérica conocida como "valor *hash*" o "huella

digital". Cada bloque de la cadena contiene el valor *hash* que validó la transacción antes de que siguiera su propio valor *hash*. Los *hash* confirman transacciones en la cadena de bloques

- Libro Mayor (*ledger*): es una base de datos donde se almacena toda la información de la red. Al distribuirse en muchos computadores, se garantiza que la información de dicho *ledger* sea muy difícil de modificar y *hackear*, agregando seguridad al modelo.
- Minar: proceso mediante el cual los bloques o transacciones se verifican y agregan a una cadena. Para ello, un minero debe usar una computadora (nodo) para resolver un problema criptográfico. Una vez que la computadora ha resuelto el problema, el bloque se considera "minado" o verificado.
- Moneda (*coin*): una moneda o *altcoin* es una representación del valor de los activos digitales generada a través de su propia cadena de bloques independiente.
- Nodo: cualquier computadora conectada a la red *blockchain*. Un nodo completo es una computadora que puede validar completamente las transacciones y descargar todos los datos de una cadena de bloques específica; mientras que un nodo "ligero" no descarga todas las piezas de los datos y utiliza un proceso de validación diferente.
- Oferta Inicial de Monedas (*Initial Currency Offering*, ICO): ocurre cuando una nueva criptomoneda vende *tokens* anticipados a cambio de capital inicial.
- *Token*: representa un activo construido en un *blockchain* existente. Están diseñados para ser únicos, líquidos, seguros y transferibles instantáneamente.

Tecnología contabilidad distribuida (*Distributed Ledger Technology*, DLT)

Esta tecnología es la base en la cual se sustenta la *blockchain*, aunque con sus diferencias. La tecnología contabilidad distribuida (*Distributed Ledger Technology*, DLT) es un sistema que consiste en el registro de transacciones de diferentes activos, en distintos sitios a la vez, sin

la existencia de una entidad o registro central encargado del almacenamiento, mantenimiento y administración general de todos los datos (Sáez, 2021). Este rasgo constituye la principal diferencia con los libros de registro comunes o tradicionales. En otras palabras, se trata de una gran red informática repartida en distintas ubicaciones, donde la confianza en los demás integrantes y en los datos que registran, resulta básica para el correcto funcionamiento y fiabilidad de la red.

La tecnología *blockchain* es un tipo de DLT, la cual incluye la figura de la cadena de bloques (rasgo no esencial de las DLT), con protocolos persona a persona (P2P) que garantizan la seguridad e invariabilidad de los datos contenidos en ellos (Maldonado, 2020; Sáez, 2021).

¿Qué es la *blockchain*?

Según Carlozo (2017), una *blockchain* es un libro de contabilidad digital de transacciones económicas que es totalmente público, transparente, actualizado de manera continua por innumerables usuarios, y considerado, por muchos, imposible de corromper, a través del cual se puede realizar cualquier tipo de operación entre dos personas sin que se requiera de ningún intermediario. Está conformada por una cadena cronológica de "bloques" en la que cada uno contiene un registro de la actividad de la red, donde la información pasa por un proceso de validación antes de ser registrada (Bogart y Rice, 2015), permitiendo unir datos protegidos criptográficamente. Estos bloques son únicos, inmutables, inalterables y dependientes del anterior, haciendo que no sea posible considerarlos en forma individual (Bullón Pérez *et al.,* 2020).

La *blockchain* permite la gestión de datos, órdenes, transacciones, derechos, propiedades, certificados, activos y unidades de valor certificada por los integrantes de la red (*tokens*), a través de un sistema de registro distribuido y descentralizado, los cuales se anotan en bloques de información secuenciales, que son compartidos colaborativamente entre muchos participantes de la red y verificados por los nodos que la

conforman, creándose un libro contable con copias idénticas en todos los nodos de la red (Puig, 2018).

Según Arrasco (2021), estas características son las que permiten la verificación de diferentes transacciones a lo largo del tiempo, generando seguridad y confianza en los datos almacenados, posibilitando la realización de diferentes acciones sin necesidad de la participación de un intermediario (como, por ejemplo, un banco) lo que también disminuye el coste de transacción.

La aplicación más conocida de esta tecnología está asociada a las monedas digitales o criptomonedas; sin embargo, existen diversos ámbitos de aplicación tanto en el sector público como en el sector privado, muchas de las cuales aún están por desarrollar.

Valores de la tecnología *blockchain*

Según destaca el Centro de Difusión del Conocimiento Económico (CEDICE Libertad, 2021), esta tecnología contempla valores especialmente apreciados en el sector público, a saber:

- Transparencia: en virtud de que la información almacenada en los bloques se encuentra disponible para los participantes de la cadena, o cualquier persona con acceso, en todo momento evitando la ocurrencia de operaciones indebidas dado que puede ser revisada por agentes externos, como organismos similares al Banco Mundial.
- Eficiencia: es posible trabajar con múltiples fuentes de datos y hacer más transparentes los trabajos colaborativos, mejorando el método de compartir datos y garantizando su seguridad, lo que aumenta la eficiencia de las operaciones y proyectos.
- Inclusión y control ciudadano: los ciudadanos pueden conocer directamente acerca de la información almacenada en los bloques, "mantenerse al tanto de las operaciones, proyectos o posibles irregularidades. Esta característica impulsa el control de los ciudada-

nos hacia sus gobernantes, fomenta la inclusión y disminuye los incentivos a incurrir en actos de corrupción" (p. 14).
- Descentralización: la tecnología descentraliza todas las operaciones y proyectos en los que se utiliza, ya que no depende de una autoridad central.

Elementos que conforman una *blockchain*

Teniendo presente que el propósito de la *blockchain* es proporcionar seguridad a los datos, desde este punto de vista Preukschat *et al.* (2017, p. 25) plantean que esto se logra mediante la combinación de tres aspectos: criptografía, estructura y consenso.

- Criptografía: mediante un algoritmo con clave de cifrado, un mensaje es transformado sin atender a su estructura lingüística o significado, de manera tal que sea incomprensible a toda persona que no tenga la clave de descifrado de dicho algoritmo. Además, es fundamental para evitar la manipulación, hurto o introducción errónea de información en la cadena de bloques y garantizar la generación de firmas e identidades digitales encriptadas.
- Estructura: actúan bajo las mismas reglas o protocolo para dar validez al bloque, y a la información recogida, e incorporarlo a *blockchain*. Una vez realizada esta tarea, la cadena continuará con la emisión del siguiente bloque, permaneciendo inalterable la información registrada por medio de la criptografía.
- Consenso: se sustenta en un protocolo común para la verificación y confirmación de las transacciones realizadas, asegurando su irreversibilidad. Así mismo, este consenso debe proporcionar a todos los participantes de la red una copia inalterable y actualizada de las operaciones ejecutadas.

Desde un punto de vista operativo, se puede hablar de que los elementos básicos necesarios para el funcionamiento del *blockchain* son: nodos, protocolo estándar, red de pares y sistema descentralizado.

- Nodos: pueden considerarse como los equipos informáticos de la red que sostiene la cadena de bloques, es decir, su infraestructura (Cabrera Valencia, 2018), siendo quien aporta su capacidad de procesamiento con la finalidad de ejecutar el trabajo de validación de los bloques de datos, los cuales se registran en la cadena a cambio de una retribución (criptomoneda). También, se pueden definir como los usuarios participantes en la red ejecutando el *software* y cumpliendo diferentes tareas de acuerdo con el tipo de nodo (Berryhill *et al.,* 2018 citados por CEDICE Libertad, 2021). Constituyen una red colaborativa de ordenadores, la cual se encarga del almacenamiento de datos, preservación de los registros y el resto de las acciones destinadas a garantizar la autenticidad de los mismos (Bullón Pérez *et al.,* 2020).

Existen diferentes tipos de nodos: nodos completos, nodos de minería y nodos ligeros. Los nodos completos participan en la red almacenando una copia de toda la información de la cadena, constatando y validando que no existan modificaciones en los bloques y remitiendo la información a otros nodos. Los nodos de minería, realizan estas mismas tareas y, además, generan nuevos bloques de información a la cadena con los datos validados por los nodos completos. Finalmente, los nodos ligeros solamente se encargan de enviar información a la cadena, para su validación y almacenamiento (CEDICE Libertad, 2021).

En función de la complejidad de la red, estos nodos pueden ser desde una computadora personal hasta una supercomputadora, donde se almacena el libro mayor de contabilidad (Cabrera Valencia, 2018). Independientemente de su capacidad, todas las unidades deben contar con el mismo protocolo para poder comunicarse entre sí.

- Protocolo estándar: corresponde al *software* informático, con el cual deben contar todas las computadoras que constituyen la red para poder comunicarse a través del mismo lenguaje. Su objetivo es lograr "un consenso acerca de cuál será la versión válida de registro y definir la comunicación entre los nodos" (Gómez-Cadiñanos,

2021, p. 21). Este consenso es clave para proporcionar la seguridad de los datos (Preukschat *et al.,* 2017).

- Red de pares (*Peer-to-peer*, P2P): es una red de pares compuesta por los distintos nodos, conectados e iguales entre sí, donde no existe jerarquía, pudiendo haber excepciones en el caso de las *blockchain* privadas (Puig, 2018).
- Sistema descentralizado: la red se controla de manera equivalente, ya que los participantes son iguales entre sí, por lo menos en las *blockchains* públicas (Puig, 2018).

Principios de funcionamiento de la *blockchain*

Según Catalini (2017), el funcionamiento de esta tecnología se sustenta en cinco principios básicos, a saber:

- Base de datos distribuida: debido a que cada parte de una cadena de bloques cuenta con acceso a toda la base de datos, incluyendo su historial completo, sin que exista una sola persona o entidad con el control sobre la información, lo cual implica que cada persona o entidad puede verificar de forma directa los registros de sus socios de transacciones, sin requerir de un intermediario.
- Transmisión de igual a igual: la comunicación ocurre directamente entre pares, cada nodo almacena y reenvía información a todos los demás nodos que constituyen la cadena de bloques.
- Transparencia con seudonimato: toda transacción y su valor asociado se encuentran visibles para cualquier persona con acceso al sistema. Cada nodo, o usuario, en *blockchain* cuenta con una dirección alfanumérica única de más de 30 caracteres que lo identifica. Todas las transacciones se realizan entre direcciones. Los usuarios pueden optar por mantener el anonimato o proporcionar prueba de su identidad.
- Irreversibilidad de los registros: cuando se ingresa una transacción en la base de datos y se actualizan las cuentas, estos registros no pueden ser modificados, debido a la vinculación que existe con todos los registros de transacciones anteriores (de ahí el término

"cadena"). Se implementan diversos enfoques y algoritmos computacionales para asegurarse de que la grabación en la base de datos sea permanente, ordenada cronológicamente y disponible a todos los demás en la red.

- Lógica computacional: las transacciones se pueden vincular a una lógica computacional y ser programadas, lo cual permite a los usuarios configurar algoritmos y reglas que activen automáticamente transacciones entre nodos, base de los contratos inteligentes (*smart contract*).

Funcionamiento de la *blockchain*

Sabiendo que se trata de un registro de transacciones que es compartido y verificado por los distintos participantes del sistema, el proceso a través del cual se desarrolla de manera descentralizada involucra los distintos elementos que se resumen a continuación:

- Los nodos conectados a la red descentralizada (*Peer-to-Peer)* se encargan de guardar la cadena completa que conforma la *blockchain*, almacenándose en cada uno de los integrantes de la red una copia idéntica (Romo Conde, 2021).
- Cada nodo emite diferente información (acerca de *Bitcoins*, alquileres, ventas, etc.), a la que se le denomina *token*, la cual viaja encriptada por la red, haciendo imposible que se revele el contenido.
- La red se compone de diferentes bloques, cada uno de los cuales contiene un conjunto de información verificada sobre diferentes transacciones. Estos bloques se generan a través de un *software* de código abierto y registran la información sobre cuándo y en qué secuencia se realizó la transacción, almacenando cronológicamente la información de las transacciones que se efectúan en la cadena. La programación de este *software* incluye las reglas que rigen la cadena (CEDICE Libertad, 2021).
- En cada bloque se recoge un código único de identificación con el bloque anterior, un grupo de transacciones y un código único de identificación con el bloque posterior.

- Un Brand Regular a vez que se realiza la operación en cuestión, un nodo se encarga de comprobar las transacciones y los *hash* correspondientes, encriptando esta información a través de funciones matemáticas, generando una huella digital única basada en el contenido de los bloques (Berryhill *et al.,* 2018), transformando el bloque una nueva serie de caracteres con una longitud fija (Maceo Herrera, 2021), es decir, se le otorga una identidad única e irrepetible al bloque llamada *hash*, además de un lugar específico dentro de la cadena.
- Cuando se agrega un nuevo bloque a la cadena, inicia un proceso en el que se le añade la información del *hash* del último bloque de la cadena (CEDICE Libertad, 2021). De esta manera, este *hash* queda registrado tanto en el bloque existente como en el nuevo integrante.
- El método de validación de la información se conoce como mecanismo de consenso, el cual "debe garantizar que todos los agentes del sistema puedan ponerse de acuerdo respecto a una fuente única de verdad, incluso en el caso de que algunos de ellos falle" (Binance Academy, 2018b). Según Bullón Pérez *et al.* (2020), en su mayoría, las *blockchains* utilizan dos métodos de validación de los nuevos bloques, antes de que sean incorporados a la cadena. La prueba de trabajo (*Proof of Work,* PoW) que utiliza datos difíciles de producir, pero fáciles de verificar para el resto, y la prueba de participación (*Proof of Stake,* PoS) en la cual la verificación queda a cargo de un nodo aleatorio, siempre que cumpla una serie de criterios. En todo caso, se prescinde de la necesidad de un intermediario (entidad financiera o entidad reguladora) en este proceso compartido de validación de la información a añadir.
    - En el caso concreto del *bitcoin*, el mecanismo utilizado para lograr el consenso es el PoW. Los diferentes "mineros" entran a competir entre ellos ante un problema criptográfico. El nodo que logra imponerse al resto recibe una recompensa en forma de *bitcoins*, además de las comisiones asociadas a tales transacciones (Romo Conde, 2021).

- También se tiene la prueba de autoridad (PoA), el cual es un procedimiento que genera tasas en menor tiempo que PoW. En consecuencia, las transacciones y los bloques son verificados por los "validadores", a través de fases automáticas que requieren de tres requisitos con la finalidad de asegurar su consistencia: verificación producida en la cadena; calificaciones complejas para el logro de incentivos y demostración coherente entre las investigaciones realizadas y los procesos propios (Grupo Garatu It Solutions, 2018).

• Es posible que la cadena pueda modificarse, ya sea por un cambio en las reglas de la red o debido a la solución de errores, lo que es conocido como bifurcación (*fork*), la cual establece la nueva manera como se trabajará la cadena a partir de ese momento, dividiendo la serie de bloques (Bolaños *et al.*, 2019). Los autores plantean que existen dos tipos de *fork*. Cuando las nuevas reglas o modificaciones son incompatibles con la versión precedente (*hard fork*), y cuando estas pueden coexistir con las anteriores (*soft fork*).

Tomando como resumen lo planteado por CEDICE (2021):

> En resumen, se puede decir que la tecnología *blockchain* es una red distribuida que utiliza los programas diseñados con DLT, donde cada usuario es un nodo distinto, tiene acceso a los bloques de información y, según las normas de la red, aun- que cada nodo realiza diferentes tareas, el resultado siempre es compartido. Se debe destacar que cada tarea se lleva a cabo de manera automática por el *software*, utilizando internet como recurso de conexión. (p. 10)

Tipos de *blockchain*

De acuerdo con los diferentes autores, las *blockchains* se pueden clasificar en función de las normas y propiedades que se establecen para la red. Así, se identifican dos categorías principales, a saber: según el nivel de apertura y según el nivel de permiso o accesibilidad.

Según el nivel de apertura de la red, se tienen las cadenas de bloques públicas, privadas, híbridas (federales o de consorcio) y *blockchain* como servicio (*Blockchain as Service*, BasS).

- *Blockchain* pública: permite que cualquiera pueda acceder, ver la información y hacer uso de ella dentro de la cadena, esto incluye datos, *software* y su desarrollo, donde cualquier individuo puede revisarlos, desarrollarlos y mejorarlos (CEDICE Libertad, 2021 y López Gómez-Cardiñanos, 2021). Basta descargar una aplicación y conectarse con una determinada cantidad de nodos. Se caracteriza por ser transparente, descentralizada, distribuida, consensuada y abierta (Puig, 2018) y pseudónima (los propietarios de las transacciones no son identificables de forma personal, siendo rastreables sus direcciones son rastreables por ser público). En tal sentido, estas cadenas no pueden ser anónimas, a excepción de las que expresamente se diseñan para ello (Preukschat *et al.*, 2017).
- La validación de la información se realiza a través de los nodos verificadores o mineros, quienes reciben una recompensa por cada una de las comprobaciones ejecutadas, además de las comisiones correspondientes a las transacciones. El sistema de remuneración depende de la regla de consenso (PoW, PoS, PoA) elegida para el sistema. Entre este tipo de cadenas se tienen *bitcoin*, *ethereum* y *litecoin* (todas basadas en la regla de consenso PoW) (Grupo Garatu It Solutions, 2018).
- *Blockchain* privada: solo puede ser vista por un grupo elegido de personas, debido a una serie de restricciones, tanto a la accesibilidad como al papel que desempeñan los participantes (CEDICE Libertad, 2021 y Carbonero del Val, 2021). Existe una única entidad central que ejerce control sobre las acciones que se ejecutan en la cadena: acceso a los usuarios para realizar las transacciones, acciones y base de datos, razón por la cual muchos usuarios no la consideran *blockchain* (Puig, 2019). Se caracteriza por ser cerrada, base de datos distribuida entre varios nodos (entre sus participantes o limitados a algunos de ellos) donde estos se conocen haciéndo-

se más propensa a la corrupción de datos, y anónima en cuanto a la posibilidad de establecer niveles de anonimato para realizar o proteger transacciones (Preukschat *et al.,* 2017). Este tipo de cadenas se utiliza para el intercambio de grandes volúmenes de datos, donde interesa mantener la reserva de la información. Las instituciones financieras son las que más han usado este recurso (Gutiérrez, 2019). Entre los ejemplos existentes, se pueden mencionar MONAX, Multichain, Blockstack, Ripple, Chain Quorum.

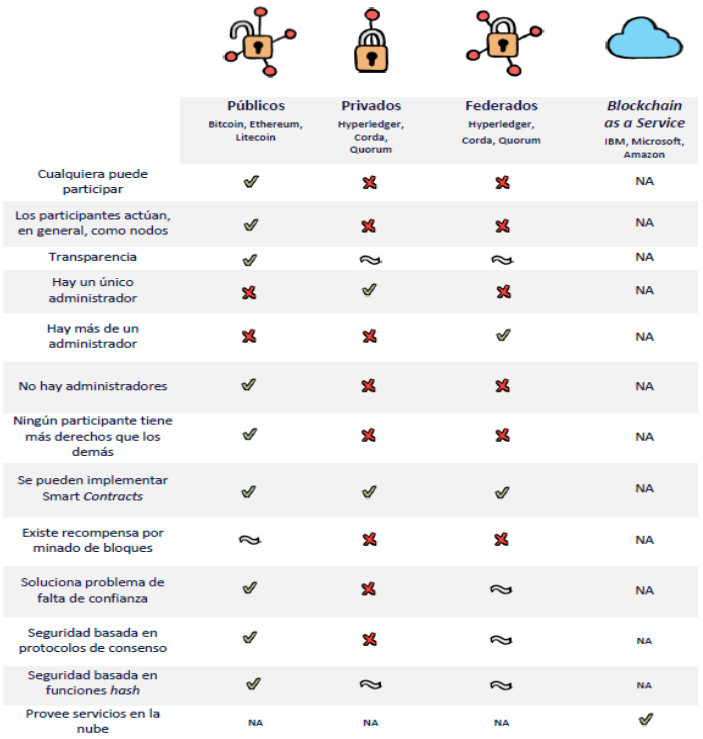
- *Blockchain* híbrida, federal o de consenso: la verificación y el encriptado de los datos es llevado a cabo por uno o varias entidades; mientras que el modelo de datos es accesible a todos con las limitaciones que estos terceros concedan a lo soliciten o, en su defecto, estará restringida solo a los participantes de la *blockchain* en ese momento. El consenso es controlado por un determinado grupo de nodos, seleccionados para tal fin (Grupo Garatu It Solutions, 2018 y Maceo Herrera, 2021). En términos generales, este tipo de cadena se utiliza por gobiernos, asociaciones y empresas (por ejemplo, del sector bancario y energético), las cuales realizan un gran número de transacciones.
- En este caso, no se asocia a criptomonedas, ni a la obtención de recompensas por el minado de los bloques (Gutiérrez, 2019). Surge con la finalidad de aprovechar los beneficios de la seguridad de la *blockchain* pública en cuanto a las dificultades para alterar los datos debido a la cantidad de nodos y la privacidad y mantenimiento controlado de la cadena privada. En definitiva, es parcialmente descentralizada y su objetivo es ofrecer un alto grado de transparencia (Maceo Herrera, 2021; Romo Conde, 2021; López Gómez-Cardiñanos, 2021).
- *Blockchain* como servicio (BasS): se refiere a una tecnología *blockchain* dispuesta en la nube, al servicio de alguna actividad. Abarca el almacenamiento de información de las transacciones, aumento de la seguridad, no requiere inversión en hardware y ofrece un entorno amigable para trabajar, siendo capaz de crear un propio canal de *blockchain* sin requerir de programación (Rodríguez, 2019).

Según el nivel de permiso o accesibilidad, se puede hablar de las cadenas de bloques abiertas (*blockchain permissionless*) en las cuales cualquier usuario puede contribuir a la generación y validación de la información, y de las cadenas de bloques cerradas o permisionadas (*blockchain permissioned*) donde solo un grupo selecto de usuarios tiene la posibilidad de realizar tales tareas (OECD, 2018).

En resumen, en la figura 1 se presenta la comparación entre los tipos de *blockchain* tomando en consideración sus diferentes características.

Figura 1

Resumen comparativo de los tipos de blockchain



Nota. Tomado de Allende y Colina (2018, p. 26).

Principales usos o funcionalidades de la tecnología *blockchain*

Esta es una tecnología que se encuentra en pleno desarrollo, por lo que el gran reto en la actualidad está en afianzar las aplicaciones existentes y, más aún, en incorporar nuevos campos de acción para aprovechar los beneficios que ofrece a los distintos ámbitos de la sociedad. Por lo que, en esta sección, se exponen solo algunos de los usos más comunes.

- Criptomonedas: son "una forma de dinero efectivo digital que permite a los individuos transferir valor en un entorno digital, siendo su principal función "actuar como un sistema de dinero efectivo electrónico que no es propiedad de ninguna parte" (Binance Academy, 2018c).
- Contratos inteligentes (*smart contracts*): se trata de acuerdos entre las partes sin que exista la necesidad de un intermediario, donde la *blockchain* se utiliza con el fin de garantizar el cumplimiento de las condiciones del contrato. Su origen se ubica en los años 90, cuando Nick Szabo los concibió "como herramientas que formalizan y protegen las redes de ordenadores mediante la combinación de protocolos e interfaces de usuarios" (Binance Academy, 2019a). En el ámbito actual, se puede considerar como acuerdos digitales de obligatorio cumplimiento al cumplirse con una serie específica de reglas, predefinida a través de un código informático, el cual será replicado y ejecutado por toda la red de nodos, prescindiendo de intermediarios.
- Almacenamiento y seguimiento de datos: se pueden crear bases de datos, las cuales se modifican y observan en tiempo real (CEDICE Libertad, 2021), con aplicaciones con propósitos tan diversas, tal como lo plantean diferentes autores (Carbonero del Val, 2021; Bolaños *et al.,* 2019; Muñoz Moreno, 2020).
    - Trazabilidad: en el rastreo de productos a lo largo de toda la cadena de suministro, incluyendo detalles de ubicación, tiempos, procedencia de materiales, distribución y venta.

- Propiedad industrial e intelectual: protección del diseño y detección de falsificaciones. Mejor coordinación entre autoridades administrativas y jurídicas.
- Planificación colaborativa: ofreciendo datos confiables y en tiempo real a los participantes de la cadena, que les permita la planificación de sus actividades de manera más eficiente.
- Sostenibilidad: aportando transparencia en la información acerca de aquellos aspectos relacionados con el consumo responsable y sostenible.

Smart contracts o contratos inteligentes

Vale la pena profundizar un poco más sobre el tema de los contratos inteligentes debido a que esta es una de las aplicaciones en la que más están invirtiendo tiempo y recursos todos los entusiastas de la tecnología *blockchain*. A pesar de su nombre "contratos inteligentes" o *smart contracts*, hay quienes dicen que no se les puede llamar "contratos" debido a que por ahora todavía no tienen la característica de ser legales, y, tampoco son "inteligentes" porque su funcionamiento requiere de la aplicación de instrucciones muy básicas, a pesar de ello, los experimentos hasta ahora realizados no han tenidos los mejores resultados.

El término *smart contract* fue acuñado por Nizk Szabo en los años noventa (Kolvart *et al.*, 2016) quien pensó que su uso podría optimizar los procesos relacionados con el comercio electrónico. Al estar basado en tecnología *blockchain* su funcionamiento también concibe en un registro de contratos de manera descentralizada. Todos los ordenadores de la red tendrán almacenado el código del programa de manera simultánea.

Su funcionamiento consiste en que un contrato inteligente se ejecutará de manera automática en el momento en el que se cumplan todas las condiciones estipuladas en el mismo sin que las partes puedan modificar los términos ni interrumpir su ejecución. Para ello, todos los ordenadores de la red estarán sincronizados al momento de la ejecución y todos ellos deberán obtener el mismo resultado al finalizarla.

Nótese que esta propuesta no requiere que exista un agente que ordene su ejecución ya que esto sucederá inmediatamente después de que se cumplan todas las condiciones. Ni siquiera los principales nodos de la red podrán evitar la ejecución.

Tal vez podamos comparar este tipo de contratos con una simple máquina expendedora de café. Si una persona desea tomar un café debe seguir los siguientes pasos:

- Depositar el dinero, si no lo hace la máquina no preparará el café.
- Escoger el tipo de café que desea, si no lo hace la máquina no preparará el café.
- Escoger la cantidad de azúcar, si no lo hace la máquina no preparará el café.
- Tomar su café de la máquina.

El ejemplo anterior es bastante sencillo, pero con él podemos darnos cuenta de que la máquina preparará el café únicamente en el caso de que las tres condiciones anteriores se hayan cumplido, además, una vez que la persona hay ejecutado los tres primeros pasos ya no podrá hacer nada para cancelar la preparación del café.

A continuación, se mencionan algunas características de este nuevo tipo de contratos:

- No pueden ser modificados ni siquiera en el caso de que una de las partes del contrato decida cancelar el contrato o modificar una de las cláusulas.
- Es incorruptible y una vez que se cumplan todas las condiciones su ejecución es inevitable.
- La ejecución de un contrato inteligente puede contemplar la transferencia de la propiedad de criptoactivos (como criptomonedas) de manera automática e irreversible.
- No requiere de un intermediario neutral que asuma el papel de un mediador entre las partes.

Además, los contratos inteligentes se ven beneficiados por la combinación de la tecnología *blockchain* con la inteligencia artificial. Una de las aplicaciones de la inteligencia artificial se centra en la inteligencia de negocios. Existen varios proyectos enfocados en desarrollar herramientas útiles para una gran diversidad de necesidades relacionadas a los negocios (Almonacid y Coronel, 2020). Por ejemplo, si un equipo auditor tendría la tarea de revisar manualmente los términos y condiciones de un contrato inteligente, una aplicación potenciada con inteligencia artificial podría hacerlo reportando errores, inconsistencias y vulnerabilidades en tan solo segundos.

Aplicaciones en distintos sectores

Si bien es cierto que la *blockchain* surge de la mano con el *bitcoin*, por lo que se asocia con transacciones de dinero digital, también es relevante su potencial de aplicación en una amplia gama de actividades en el sector privado, público y organizaciones no gubernamentales (ONG), tal como lo señalan autores como Maceo Herrera (2021), Carbonero del Val (2021), Muñoz Moreno (2020), Linares-Barbero (2019), Berryhill *et al.* (2018), CEDICE Libertad (2021), López Gómez-Cardiñanos (2021), entre otros, y se resumen en los siguientes aspectos:

- Transacciones financieras: permite ejecutar con mayor rapidez las transacciones con respecto a los métodos bancarios tradicionales, siendo la aplicación más consolidada de la *blockchain*.
- Automatización de la gestión de pagos y cobros, de forma simultánea: con condiciones acordadas entre múltiples participantes y previstas en contratos inteligentes, inmediatamente después de que un servicio haya sido completado.
- Comercio exterior: en automatización de los procesos entre diversos actores involucrados (compañías importadoras, exportadoras, aduanas, transportes, puertos, etc.), donde la utilización de *smart contracts* agilizaría los trámites, impulsando la competitividad.

- Ciberseguridad: en el que cada contrato almacenado dentro de la red distribuida tiene asociado un código de almacenamiento en la *blockchain*, el cual está encriptado con algoritmos seguros, lo que obstaculiza la posibilidad de cometer alguna modalidad de fraude o eliminación de los mismos.
- Telecomunicaciones: el impacto de esta tecnología en este sector económico puede ser especialmente significativo en la gestión interna de las redes, cualquier control automático o autorregulación, al reducir la complejidad de tales tareas. La evolución de la 5G, en conjunto con estructuras de redes flexibles, distribuidas y adaptables, permitirán definir diferentes tipos de redes dentro de la misma infraestructura. Esta combinación permitirá satisfacer los requerimientos técnicos demandados por los diferentes sectores, como la industria de automóviles autónomos o servicios de salud remota.
- Proveedores de servicio de Internet (ISP): podrían contar con una su red que permitirá a sus clientes demandar más recursos, cambiar la topología, ya que la *Blockchain* detectará inequívoca e inmediatamente a quien lo solicita y, en consecuencia, realizará las acciones requeridas basado en los permisos y recursos.
- Propiedad Industrial, propiedad intelectual y falsificaciones: la *blockchain* sería un avance para la protección de la propiedad industrial e intelectual, apoyando el registro de marca, manteniendo datos que permitan avalar titularidad de diseños (en fecha y hora), demostrar el momento de creación y de primera venta, facilitando la labor de documentación de las pruebas, inmediatez y ahorro en costos, utilizando los contratos inteligentes para las licencias de marca y cobro de derechos (Muñoz Moreno, 2020) y posibilitando a los consumidores para constatar la originalidad de los productos al combinarla con otras plataformas, como las de las etiquetas de identificación por radiofrecuencia utilizadas en el sector alimenticio (Linares-Barbero, 2019).

- Trazabilidad: permitiría el rastreo de los productos a lo largo de todas las actividades que conforman la cadena de suministro, pudiendo incorporarse detalles acerca de la ubicación y tiempo exacto de la producción, introducir indicadores de sostenibilidad como la procedencia de los materiales utilizados en la producción, distribución y venta (Muñoz Moreno, 2020).
- Sostenibilidad: permitiría comprobar si las materias primas provienen de un comercio justo, si los materiales ecológicos efectivamente lo son, o si se ha cumplido con los procesos de reutilización y reciclaje de materiales.
- Servicio público: la recomendación para instituciones proveedoras de servicio público son las redes *blockchain permissioned* con una combinación de acceso público y privado, ya que permiten diseñar una plataforma con diferentes tipos de agentes, desde un ciudadano que busca un servicio y registra sus datos con ese fin, hasta instituciones que requieran distintos segmentos de la información para trabajar) (Berryhill *et al.,* 2018). En este sentido, la OCDE señala que las aplicaciones más comunes en los servicios públicos son las que ofrecen una plataforma para registrar información de los usuarios:
  - Registros de identidad: como documentos de identidad, certificados de nacimiento, licencias de conducir, registros de boda, pasaportes, visas.
  - Registros personales: como registros médicos, registros criminales, registros financieros y crediticios, registros de propiedad, registros de pensión y ayuda social, registros de calificaciones y educación.
  - Registros de servicios: Como el consumo de energía, agua e internet, acceso a bienes básicos como alimentos, medicamentos y ropa.

En estos casos destaca la importancia de la segmentación de la información y el acceso que tengan los participantes en la cadena.

- Representaciones digitalizadas de documentos tradicionales de identidad: tales como licencias de conducir, pasaportes, certificados de nacimiento, registros de seguridad social, entre otros (Maceo Herrera, 2021).
- Identidad digital: constituiría la base para la integración de todos los servicios, la cual sería indispensable para ofrecer y recibir los mismos en hospitales, escuelas, bancos, empresas de electricidad, agua, telecomunicaciones, transporte, etc. (Maceo Herrera, 2021).
- Historia médica: incluiría registros médicos, farmacéuticos, consultas, tratamientos y datos de utilización de dispositivos médicos. En este último sería fundamental el registro de todos los procedimientos realizados durante una intervención quirúrgica con la asistencia de dispositivos dotados del Internet de las cosas (*Internet of things*, IoT).
- Gestión de cobros o pagos de los servicios, como pagos de peaje por autopistas, abastecimiento de combustible o pagos de factura de electricidad.
- Seguimiento de sus inventarios y donaciones en ONG y proyectos públicos: esta tecnología permitiría hacer un seguimiento de sus inventarios y donaciones, con el registro cronológico de la procedencia de un bien, su almacenamiento y, finalmente, su consumo. Además, existiría un uso único de la cadena de bloques para los fondos y proyectos públicos, haciendo transparente las transacciones, permitiendo ciudadanos y otras instituciones conozcan y verifiquen la manera como se utilizan los recursos (CEDICE Libertad, 2021).
- Internet de las cosas: estos dispositivos son fundamentales como complemento a la tecnología *blockchain*, ya que harán posible la comprobación automática de cláusulas establecidas en los contratos inteligentes, logrando acelerar, abaratar y optimizar la realización de las transacciones y el funcionamiento del *blockchain*. Los dispositivos inteligentes que envíen información a la cadena de bloques deberán contar con una identidad digital que les permita firmar digitalmente dicha información, para garantizar su confiabilidad (Maceo Herrera, 2021 y López Gómez-Cardiñanos, 2021).

Proceso de aplicación de tecnología *blockchain* en los proyectos

Los distintos aspectos asociados a la tecnología son aún desconocidos para la mayoría de las organizaciones (públicas o privadas), por lo que CEDICE Libertad (2021), ha esbozado un proceso con la finalidad de apoyar su utilización en sus proyectos, la cual se detalla a continuación:

Paso 1. Bosquejar el proyecto: se debe planificar el proyecto donde será utilizada la *blockchain,* definiendo qué se busca ofrecer o solucionar, delimitar elementos necesarios para alcanzar los objetivos, agentes involucrados y recursos disponibles para el proyecto. Por esta razón, es necesario previamente haber identificado el problema, contexto, personas afectadas y agentes intervinientes, condiciones como institución organizadora, limitaciones y capacidades técnicas para el programa y las leyes o normativas que involucran al proyecto.

Paso 2. Evaluar la aplicabilidad de *blockchain*: es necesario evaluar la efectividad de la cadena de bloques, y para ello se recomienda utilizar el diagrama presentado en la figura 2, cuyo objetivo es identificar si la tecnología *blockchain* es la herramienta más eficiente para el proyecto, ya que existen alternativas que pueden brindar mejores soluciones para ciertas tareas.

Paso 3. Ayuda profesional: contactar a quién será encargará de aplicar la cadena de bloques como herramienta para alcanzar los objetivos, ya sea contratando en la organización un equipo de programadores con experiencia en proyectos similares, o adquiriendo un servicio de terceros. La última alternativa cuenta con la ventaja de tener acceso a la experiencia de estos agentes en proyectos *blockchain*, facilitando el trabajo y aprovechando sus sugerencias para el proyecto.

Paso 4. Prueba de concepto (***Proof of concept***, PoC) ***blockchain***: en esta etapa se instrumenta, junto a los expertos, un proceso de planificación para determinar el uso de esta tecnología en el proyecto, identificando

las características únicas requeridas (normas del programa y funciones de los agentes involucrados), se establece el tipo de *Blockchain* que funciona con el proyecto (acceso público o privado, manejo de información *permissioned* o *permissionless*). Su objetivo es delimitar la aplicación de esta tecnología en el proyecto, "concretando las ideas de la institución organizadora con el apoyo del equipo de programadores y dándoles forma dentro de la cadena… (y) permite conocer de forma preliminar los posibles recursos que requiere" (p. 18).

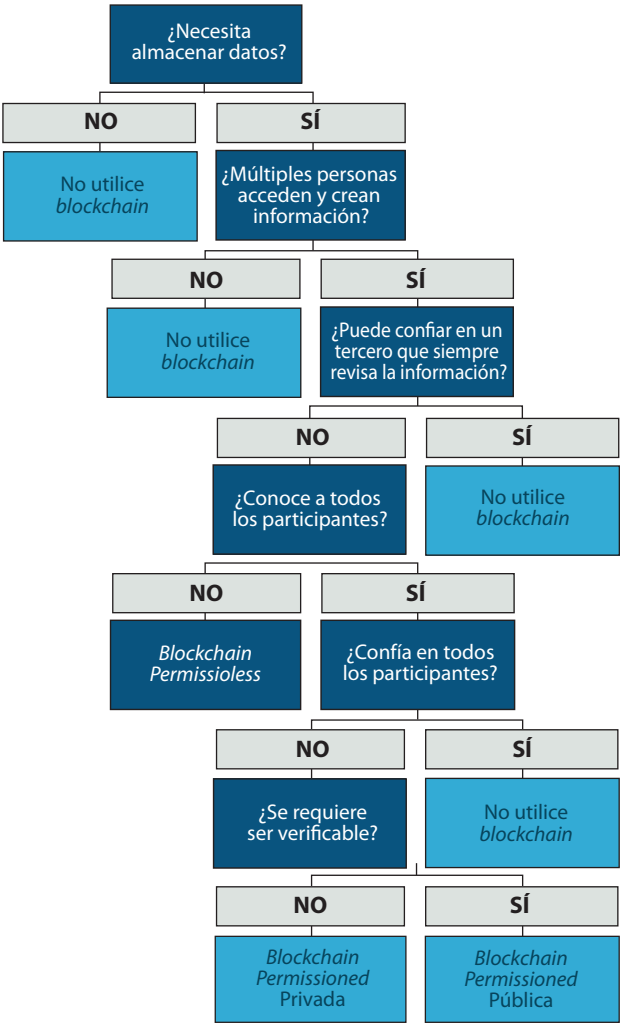
Paso 5. Producto mínimo viable: se hace una prueba del funcionamiento de la cadena, comprobando la eficiencia del programa para alcanzar los objetivos del proyecto y evaluando los costos que requiere en el tiempo para la sostenibilidad del servicio. Esto permite identificar la necesidad de realizar modificaciones antes de hacer público el programa, probándose el proyecto internamente en la institución o con la participación de un grupo selecto de usuarios y recopilando sus comentarios acerca de la experiencia. Para obtener resultados útiles, es importante definir con anticipación qué se busca evaluar con el producto mínimo viable, poniendo a prueba elementos particulares y facilitando su medición.

Paso 6. Aplicar modificaciones: se deben realizar los ajustes necesarios para lograr que el proyecto funcione eficientemente. Este paso abarca hacer cambios internos en la organización, actualizar aplicaciones asociadas a la nueva cadena, modificaciones en leyes (dependiendo de la institución organizadora) y los servicios que busque ofrecer. Una vez incorporados estos cambios, se repite el paso 5, con el objetivo de identificar la efectividad de las modificaciones y la existencia de otros aspectos a corregir.

Paso 7. Publicar el proyecto y actualizarlo: por último, se procede a permitir el acceso del público al proyecto y permanecer en constante contacto con las personas a fin de evaluar su satisfacción para evaluar si es necesario introducir modificaciones, volviendo a los pasos 5 y 6 antes de proceder a actualizar el programa al que tienen acceso.

Figura 2

Diagrama para evaluación de aplicabilidad de la tecnología blockchain en un proyecto



Nota. Tomado de CEDICE Libertad (2021, p. 17).

Ventajas y desventajas de la *blockchain*

Como es habitual, toda tecnología conlleva ventajas y desventajas que deben tenerse en cuenta al momento de su aplicación. En tal sentido, los siguientes son los aspectos más importantes relacionados con la cadena de bloques (Binance Academy, 2018d).

Ventajas

- Naturaleza distribuida: como los datos de una *blockchain* se almacenan en miles de dispositivos en una red distribuida de nodos, el sistema y los datos son altamente resistentes a fallos técnicos y ataques maliciosos. Cada nodo es capaz de replicar y almacenar una copia exacta de la base de datos y, en consecuencia, la desconexión de uno o más nodos no afecta la disponibilidad de la información ni la seguridad de la red.
- Estabilidad: una vez los datos se han registrado en la *blockchain*, es en extremo difícil eliminarlos o cambiarlos, haciendo que esta tecnología sea ideal para el almacenamiento de registros financieros o cualquier otro tipo de datos que requieren pistas de auditoría (trazabilidad), ya que todos los cambios son rastreados y permanentemente registrados en un libro contable (*ledger*) distribuido y público.
- Sistema *Trustless* (no requiere confiar en terceros): cuando se utiliza tecnología *blockchain*, no es necesaria la intervención de un intermediario para la realización de las transacciones debido a que la red de nodos distribuida se encarga de verificarlas mediante un proceso denominado minado, evitando el riesgo de tener que confiar en una organización individual y reduciendo los costos generales y comisiones por transacción.
- Compatibilidad con otras herramientas y plataformas: es compatible con otras herramientas y plataformas, permitiendo que el programa de la cadena acceda a información almacenada en otras plataformas, como bases de datos tradicionales u otras *blockchains*, o en caso

inverso, brinde información a externos, generando un ambiente de trabajo híbrido (Berryhill *et al.,* 2018; Lindman *et al.,* 2020).

Desventajas

- Ataques del 51 %: existen algunos tipos de ataques potenciales que se pueden presentar contra las *blockchains*, siendo uno de los más debatidos el relacionado con el algoritmo de consenso PoW que protege la cadena de bloques de *bitcoin*. Este tipo de ataque puede darse "si una entidad logra hacerse con el control de más del 50 % del *hashing power* (o tasa de *hash*) de la red" (Binance Academy, 2018d), permitiéndole eventualmente desorganizar la red a través de la exclusión o modificación intencionada del orden de las transacciones. Aunque este es un riesgo posible desde un punto de vista teórico, nunca se ha producido con éxito. A medida que la red crece, la seguridad se incrementa, resultando bastante improbable que los mineros empleen grandes cantidades de dinero y recursos en atacar *bitcoin*. En todo caso, una intervención de esta naturaleza solo podría modificar las transacciones más recientes durante un corto tiempo, debido a que los bloques se vinculan mediante pruebas criptográficas, donde la modificación de los bloques más antiguos requeriría niveles inasequibles de potencia computacional.
- Modificación de datos: una vez que se añaden los datos a los bloques, es muy difícil modificarlos. Aunque la estabilidad es una de las ventajas de las *blockchains*, en ocasiones puede requerirse cambiar o corregir alguno. El cambio de datos o código es habitualmente muy complicado y, a menudo, requiere de una *hard fork* abandonando una cadena y una nueva es retomada.
- Claves privadas: la *blockchain* utiliza criptografía de clave pública (también denominada asimétrica) para otorgar a los usuarios la propiedad de las unidades de su criptomoneda (o cualquier otro dato de la cadena de bloques). Cada cuenta de la *blockchain* (o dirección) dispone de dos claves: una clave pública (que se puede compartir) y una clave privada (que debe mantenerse en secreto). Los usuarios

necesitan sus claves privadas para acceder a sus fondos, actuando como su propio banco. Si un usuario pierde su clave privada, perderá también su dinero, sin poder hacerse nada al respecto.

- Ineficiencia: las *blockchains*, en especial las que usan PoW, son altamente ineficientes. Dada la competitividad del minado y que solo hay un ganador cada diez minutos, el trabajo de los demás mineros se desperdicia. El aumento de la potencia computacional de los mineros para tener mayores probabilidades de encontrar el *hash* de un bloque válido ha incrementado considerablemente los recursos utilizados por la red *bitcoin*, al punto de que en la actualidad consume más energía que muchos países como Dinamarca, Irlanda o Nigeria.
- Almacenamiento: los libros contables (*ledgers*) de la cadena de bloques pueden crecer mucho con el paso del tiempo. La de *bitcoin* requiere actualmente alrededor de 200 GB de almacenamiento. El actual crecimiento del tamaño de la *blockchain* parece estar superando al de los discos duros, por lo que existe el riesgo de que la red pierda nodos si el *ledger* se vuelve demasiado grande para ser descargado y almacenado por individuos.
- Infraestructura de telecomunicaciones: la implementación a gran escala de la tecnología necesitará de una infraestructura de telecomunicaciones capaz de suplir los requerimientos del servicio entre todos los participantes de la red (Maceo Herrera, 2021).

En resumen, la tecnología de *blockchain* se encuentra en pleno desarrollo, con un amplio potencial de aplicación en una variedad de sectores, industrias y actividades, cuyas virtudes pueden realizar aportes importantes en materia de transparencia y seguridad, especialmente en el manejo de recursos ámbito de lo público y organizaciones no gubernamentales.

Sin embargo, no está exenta de debilidades y riesgos. Temas como el anonimato (o seudoanonimato), la ineficiencia en la utilización de los recursos particularmente los energéticos, la inversión en adquisición en infraestructura tecnológica y la accesibilidad real de personas e instituciones para incorporarse a esta nueva dinámica, están apenas por empezar.