FORMATO PARA EL DESARROLLO DE COMPONENTE FORMATIVO

| PROGRAMA DE FORMACIÓN | Blockchain en criptomonedas |
| --- | --- |

| COMPETENCIA | 210301089 - Asesorar consumidor financiero de acuerdo con normativa y guía técnica. | RESULTADOS DE APRENDIZAJE | 210301089-01 - Identificar la aplicación de Blockchain de acuerdo con las necesidades del sector.  210301089-02 - Comprender la aplicación del Blockchain en inversiones financieras. |
| --- | --- | --- | --- |

| NÚMERO DEL COMPONENTE FORMATIVO | CF001 |
| --- | --- |
| NOMBRE DEL COMPONENTE FORMATIVO | Fundamentos, aplicación y análisis del Blockchainen el ámbito financiero |
| BREVE DESCRIPCIÓN | La tecnología Blockchainsurge como respuesta a la necesidad de digitalizar las transacciones comerciales. Ya se vienen realizando transacciones soportadas en Blockchain, gracias a que esta responde a criterios de operatividad que garantizan la trazabilidad, la seguridad, la centralización y el anonimato; sumado a que, con la criptografía apropiada y la redistribución de datos, la información queda consignada en los diferentes bloques. |
| PALABRAS CLAVE | Blockchain, criptografía, criptomonedas, *trading*, transacciones, *token* |

| ÁREA OCUPACIONAL | 1 - Finanzas y administración |
| --- | --- |
| IDIOMA | Español |

1. **Tabla de contenidos**

**Introducción**

**1. Blockchain**

1.1. Características

1.2. Arquitectura

1.3. Casos de éxito

1.4. Elementos que configuran el Blockchain

**2. Criptografía**

**3. Criptomonedas**

**4. Trading**

**5. Limitaciones y control de Blockchain**

**Síntesis**

1. **Introducción**

La transformación digital ha irrumpido en cada rincón del planeta y se hizo más notoria, dando continuidad a los nuevos modos de vida que se volvieron el cotidiano de todos con la aparición de la pandemia en el año 2020. Lo invitamos a ver el siguiente video que lo introducirá a la temática a abordar:



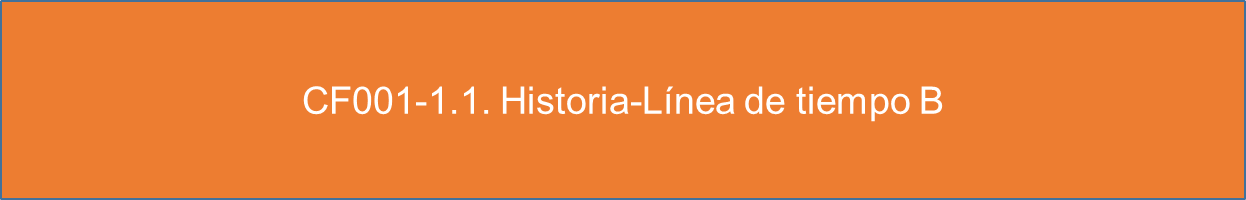
1. **Desarrollo de contenidos** 
   * + 1. **Blockchain**

La tecnología Blockchain es la digitalización de las transacciones comerciales soportada en un sistema entrelazado que, desde un criterio de consolidado o bloque, se inicia con un *hash* o valor único que lo identifica criptográficamente; por tanto, los bloques siguientes estarán identificados de la misma manera, pero vinculados, porque el bloque subsiguiente tiene una referencia al bloque anterior, lo cual garantiza que están entrelazados. Así, las operaciones comerciales que se realizan se comunican a todos los nodos de la red. De esta manera, se constituye la cadena de bloque o Blockchain, lo cual genera un *ledger* o libro contable público compartido también en todos los nodos de la red.

Para acceder a cada bloque, es necesario contar con los mensajes o claves correspondientes, a los cuales solo accederán los autorizados, haciendo uso del anonimizado; estas operaciones son confirmadas cuando hacen parte de un bloque añadido, el cual debió ser minado o, en términos técnicos, calcular su *hash*, lo cual genera un nivel de dificultad por el alto consumo de recursos informáticos que debe reajustarse periódicamente, adaptándose a la capacidad de la red, siendo complejo su cálculo al momento en que la potencia de los computadores conectados aumenta, lo que impide alterar la información contenida en uno o varios bloques, porque necesariamente debe modificarse su criptografía y esto rompe el ciclo o encadenamiento de los bloques, lo que en consecuencia genera una ruptura de la cadena y repararla es prácticamente imposible debido a su cualidad de inalterabilidad de la información y la trazabilidad que vincula**.**



Con lo ya visto, sería un desacierto profundizar en Blockchain sin conocer su origen; por esa razón, inicie conociendo parte de la historia de su nacimiento:



* 1. **Características**

La tecnología de cadena de bloques está siendo implementada en el mundo entero, gracias a su demostrada solidez, que garantiza la veracidad y transparencia de las transacciones comerciales, debido a que posee las siguientes características:

* **Inmutable:** Los registros almacenados en ella no se pueden alterar, ya que toda la red tiene una copia del 100% de los registros y se pueden validar por consenso.
* **Seguridad mejorada:** Dado que todos los nodos de la red tienen una copia de los registros, no hay forma de cambiarlos y no es posible emitir una nueva versión de un registro ya existente que cumpla con los criterios de validación por la red de nodos. No se requiere una autoridad central validadora.
* **Registros distribuidos:** Se reduce dramáticamente la necesidad de una alta capacidad de cómputo, excepto en la minería de un criptoactivo.
* **Eliminación de intermediarios:** Las transacciones son entre los participantes de la red. Por ejemplo, la autenticación de un título universitario sucede entre quien lo consulta y el dueño del título, o de un usuario mediante autorización del titular.
* **Transparencia y trazabilidad de la información:** Es posible ir hasta el origen de la primera transacción realizada sobre un elemento o documento, de manera que se puede conocer con claridad el histórico de la cadena de información contenida en un bloque.
* **Anonimato:** Se puede gozar de total anonimato, dependiendo de la necesidad puntual de la aplicación.

Para profundizar en las características de la tecnología Blockchain, lo invitamos a ver el siguiente video:



**Video: ¿Qué es y cómo funciona Blockchain?**

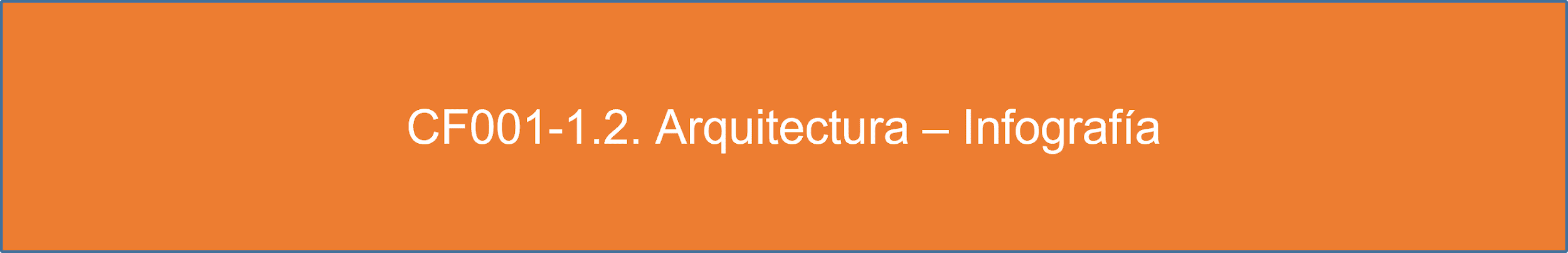
Conoce más sobre el Blockchain y su estructura. **Ver**

* 1. **Arquitectura**



Las transacciones de Blockchain ocurren dentro de una red *peer-to-peer* de computadoras distribuidas globalmente (nodos).

Cada nodo conserva una copia de la cadena de bloques y contribuye al funcionamiento y la seguridad de la red sin la intermediación de un tercero. Conozca más sobre su arquitectura:



Para ampliar la información acerca de la estructura de Blockchain*,* a continuación, se aporta el siguiente video:



**Video: ¿Cómo es la Arquitectura del Blockchain?**

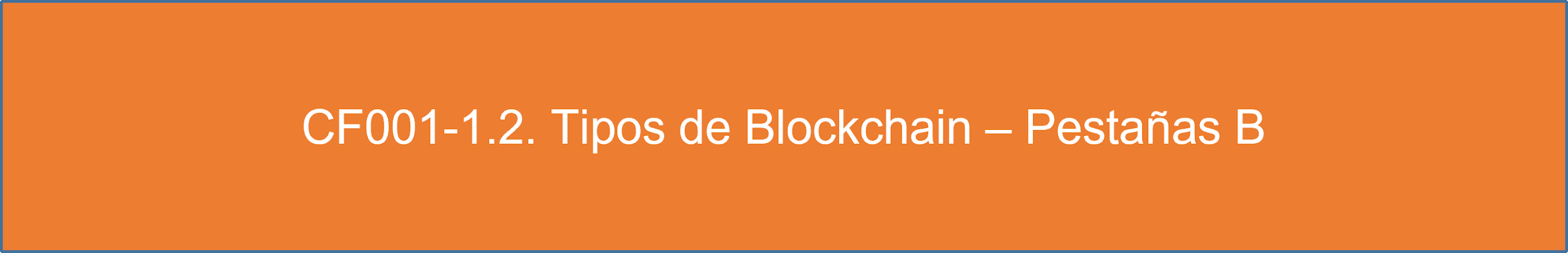
Conoce más sobre cómo está compuesto el Blockchain. **Ver**

**Tipos de Blockchain**



De lo que se ha desarrollado hasta este momento sobre el Blockchain, hay cuatro tipos principales de redes, cada una adecuada para diferentes propósitos.

A continuación, se encuentran los diferentes tipos y las características que los diferencian:



Por último, observe el siguiente cuadro, donde verá las diferencias entre cadenas de bloques:

**Tabla 1**

*Diferencias entre cadenas de bloques cerrada y abierta, a partir de características comunes*

| ***Centralización*** | ***No propietario o administrador*** | ***Tiene algún grado de administración o control externo*** |
| --- | --- | --- |
| *Acceso* | *Cualquiera puede unirse.* | *Solo los participantes preadmitidos se pueden unir a la red.* |
| *Nivel de confianza* | *Los miembros de la red no están sujetos a confiar en los otros.* | *Requiere un mayor grado de confianza entre los integrantes (porque la colaboración entre ellos puede alterar el registro).* |
| *Apertura* | *El libro es abierto y transparente, compartido entre todos los miembros de la red.* | *Son posibles diferentes grados de apertura y transparencia en el registro en el libro.* |
| *Seguridad* | *Se consigue a través de una amplia distribución en una red de gran escala.* | *Se distribuye entre el control de acceso en conjunto con DLT en redes de menor alcance.* |
| *Velocidad* | *El lento procesamiento de las transacciones restringe su volumen.* | *Mayor procesamiento de transacciones permite un mayor volumen de estas.* |
| *Identidad* | *Identidad del usuario oculta o protegida por seudónimos.* | *El administrador verifica la identidad de los intervinientes.* |
| *Consenso* | *Requiere PoW como consenso.* | *Es posible una variedad de mecanismos de consenso (típicamente más fáciles y de menos costos que PoW).* |
| *Activos* | *Típicamente criptomonedas, pero admiten la presentación de tokens que pueden equivaler a cualquier activo.* | *Cualquier activo.* |
| *Propiedad legal* | *Preocupaciones legales por la ausencia de propiedad, porque no hay entidades legales en control del libro.* | *Mayor claridad legal sobre la propiedad porque el propietario o administrador por lo general es una entidad legal.* |
| *Ejemplos* | *BigCoin, Ethereum.* | *R3’s Corda, Hyperledger Fabric.* |

Nota. Adaptación de Noriega (2021).

* 1. **Casos de éxito**

Un caso de éxito en Colombia es la implementación de esta tecnología para una instancia del Estado colombiano (la Procuraduría General de la Nación), con recursos del Banco Interamericano de Desarrollo (BID), con el que se inició el desarrollo del proyecto, desarrollando importantes alianzas público–privadas con la Universidad Nacional de Colombia, Vivelab Bogotá, Colombia Compra Eficiente, la Alcaldía de Medellín y el apoyo articulador del Centro de la Cuarta Revolución Industrial de San Francisco y de Colombia. Entidades junto a las cuales, se buscó aplicar la tecnología Blockchain en la contratación estatal, para contribuir en reducir la corrupción a través de transparencia en el proceso de licitación pública y de alertar por parte de la sociedad civil, organizaciones y ciudadanía dirigidas a la Procuraduría General de la Nación a través de un piloto utilizando esta tecnología y contratos inteligentes para poder contar con registros de información inmodificables durante el proceso de licitación pública.

Observe en la siguiente tabla las principales características de este caso de éxito:

**Tabla 2**

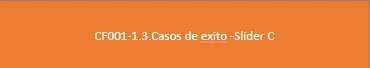
*Estructura del Blockchain para licitaciones públicas Procuraduría General de la Nación*

Interfaz de usuario gráfica, Texto, Aplicación, Word

Descripción generada automáticamente

Nota. Basada en Espinosa (2020).

Como este, existen en el mundo diferentes casos de éxito en su implementación, para lo cual, hará un pequeño recorrido:



Como ha visto en este pequeño viaje, las proyecciones del Blockchain son grandísimas. En los últimos tiempos, se ha visto la utilización de la cadena de bloques para la votación en un proceso de elección; en el sector de aseguramiento, con el fin de reducir los altos costos de intermediación; en el sector salud, se utiliza esta tecnología para mantener la historia clínica del paciente en cadena de eventos, lo cual facilita el tratamiento, especialmente, en los casos donde ocurren accidentes inesperados; y la mayor parte de sus aplicaciones son los contratos inteligentes que ya revolucionaron al mundo con su uso y que seguirán generando nuevas condiciones de operatividad que permitan mejorar su eficacia en cuanto a seguridad, convirtiéndolo en una herramienta para garantizar el cumplimiento.

* 1. **Elementos que configuran el Blockchain**

Dentro de los elementos que caracterizan la tecnología Blockchain y que garantizan su promesa de operación, hay varios que no se han abordado lo suficiente y que configuran el uso de esta tecnología, por lo cual, se hace necesario hacer un abordaje que permita seguir profundizando en el uso, estructura y aplicabilidad del Blockchain y sus proyecciones en diferentes campos. Observe algunos de estos elementos:



1. **Criptografía**

La criptografía se encarga de cifrar o codificar mensajes para evitar que su contenido pueda ser leído por un tercero no autorizado; es decir, el cometido principal de esta disciplina es la generación de códigos y algoritmos de cifrado que buscan ofuscar la información y protegerla de "ojos curiosos".

También es considerada una ciencia que apunta hacia la seguridad de los datos y los documentos; para ello, utiliza códigos o claves que permiten almacenar información secreta que, sin embargo, pueda circular por medios públicos o privados y que solo la conocerán el emisor y el receptor, siempre y cuando sepan cómo traducir la información para entenderla o cómo cifrarla para que otros no la comprendan. (Medina, 2017)

Para comprender su evolución, es necesario ver todo lo que ha sucedido desde sus orígenes:



Ya luego de conocer la historia desde su nacimiento, es bueno hacer unas aclaraciones sobre dos conceptos parecidos, pero que no significan lo mismo: la criptografía y el criptoanálisis.

* **Criptografía:** se encarga de estudiar las técnicas del cifrado de la información.
* **Criptoanálisis:** se dedica a todo lo contrario, es decir, a descifrar o decodificar esa información.

A continuación, se muestra lo que sucede cuando se envía un mensaje, este se cifra, y continúa su viaje como un criptograma, o sea que hace referencia al mensaje cifrado, es decir, que no es entendible por quien no conoce la clave para descifrarlo.

En ese trayecto, el mensaje cifrado, o criptograma, puede sufrir dos eventos, el uno, que llegue al receptor y lo descifre, o que el mensaje sea interceptado y los intrusos lo desencripten y puedan leer el mensaje.

**Figura 1**

*Ciclo del mensaje secreto*

Texto

Descripción generada automáticamente

Nota. Tomada de Medina (2017).

**Tipos de criptografía y su uso**

Los tipos de criptografía se clasifican en **clásica**, dividida en transposición y sustitución, y **moderna**: asimétrica y simétrica, y esta última se divide en bloques y flujo. En el siguiente gráfico, se pueden identificar con mayor claridad.

**Figura 2**

*Clasificación de la criptografía*

Interfaz de usuario gráfica, Texto, Word

Descripción generada automáticamente

Nota. Tomada de Medina (2017).

Para entender mejor la criptografía, es importante conocer algunos términos comunes:

* **Criptografía:** arte de cifrar y descifrar información, usando técnicas que permitan intercambiar mensajes de forma segura, pudiendo solo ser leídos por los destinatarios elegidos, sin importar si el mensaje es a través de un medio inseguro o público.
* **Cifrado:** es el proceso mediante el cual la información es transformada a través de un algoritmo que cifra la misma, por lo cual se necesitaría de una clave que permita descifrar el algoritmo.
* **Algoritmo o criptografía simétrica:** permite la encriptación y desencriptación de información mediante una llave o clave, siendo seguro y de fácil transmisión.
* **Algoritmo o criptografía asimétrica:** permite la encriptación y desencriptación de información a través de diferentes llaves o claves. La información se encriptará con una clave pública y se desencriptará con una privada. Para hacerlas seguras, pueden tener muchos bits, lo que puede hacer los procesos lentos.
* **Criptosistema:** es el procedimiento mediante un algoritmo con clave, transforma un mensaje en información comprensible, a menos que ya los receptores tengan la clave para desencriptar.
* **Esteganografía:** procedimiento que permite esconder información para que pase inadvertida; puede estar a simple vista y aún así no poder percatarse de que existe un mensaje.
* **Criptoanálisis:** es la oposición a la encriptación, es el estudio de métodos para poder descifrar o encontrar el sentido de información antes cifrada.
* **Métodos criptográficos:** son los métodos para la encriptación de información.

Dentro de los usos cotidianos que se le dan a la criptografía, se pueden encontrar los siguientes:

a. Para firmas digitales.

b. Para certificados digitales.

c. Para sistemas de autenticación.

d. Para el correo electrónico seguro.

Como ya ha visto, el cifrado y el descifrado son procesos que transforman la información por medio de un algoritmo de cifrado, y para poder descifrarla, se requiere de la clave secreta del algoritmo.



1. **Criptomonedas**

Las criptomonedas son una de las muchas aplicaciones del Blockchain, se caracterizan por ser un activo digital cuyas transacciones se realizan entre usuarios anónimos mediante una clave pública. Todo usuario maneja una clave privada (única por usuario) y una clave pública, que es la que se comparte con los demás usuarios de la red (Dwyer, 2014).

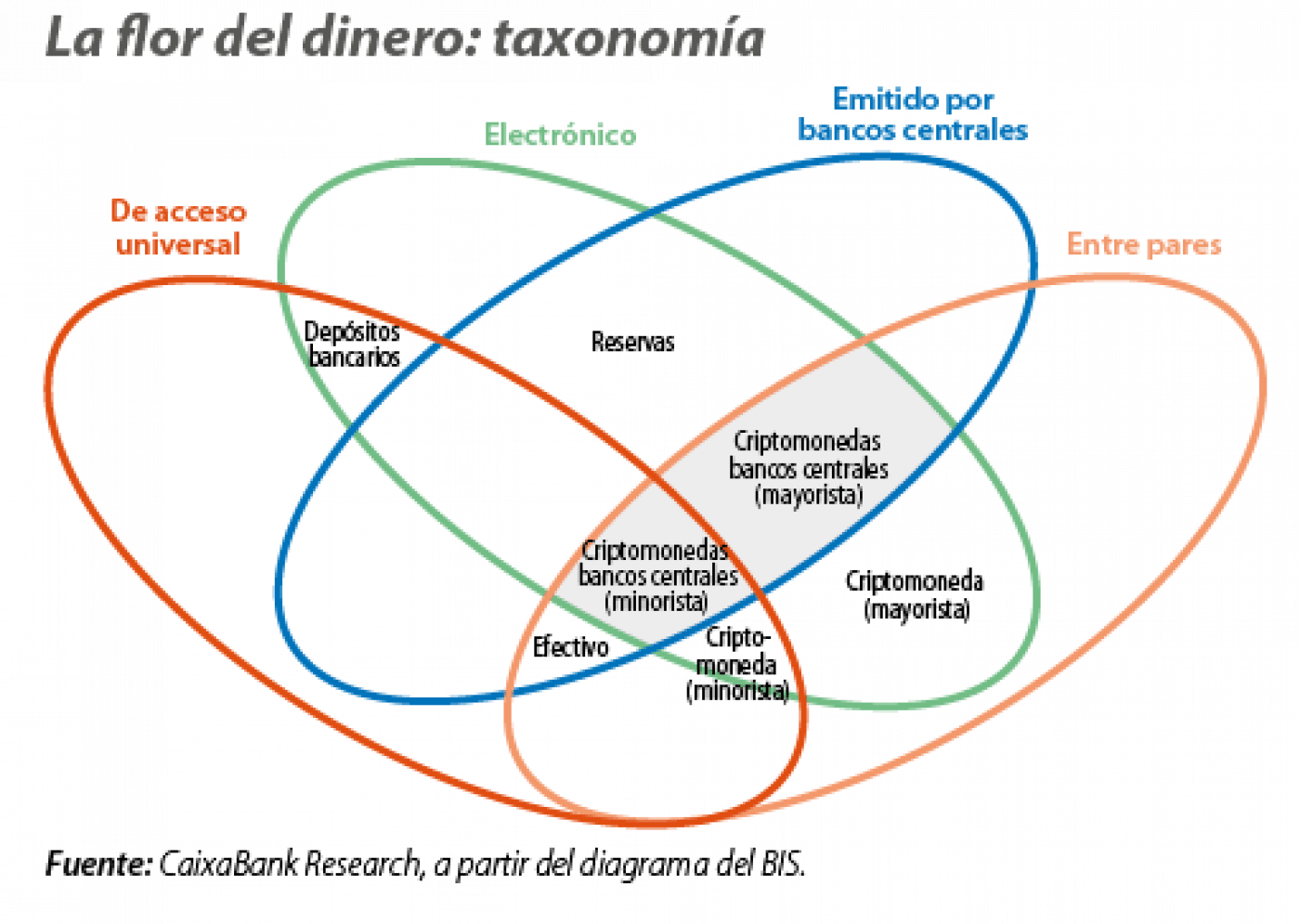
Existen varios tipos de criptomonedas, entre las que se destacan el Bitcoin y el Ethereum.



De acuerdo con el *Committee on Payments and Market Infrastructures*, las criptomonedas no son iguales, estas se asemejan porque son digitales y no requieren intermediación para su transacción, pero existen muchos tipos de criptomonedas, tal como se pueden clasificar de acuerdo con la **flor del dinero**. Existen diferencias marcadas de una criptomoneda a otra, por ejemplo: el tipo de emisor, mecanismo de transferencia, accesibilidad, forma, etc.

**Figura 3**

*Flor del dinero: Taxonomía*



Nota. Adaptada a partir de Caixa Bank Research (2019).

La tecnología Blockchain se basa en tres elementos esenciales, que son:

**tecnología de libro mayor distribuido, registros inalterables y contratos inteligentes.**

Estos elementos se basan en el principio de transparencia, debido a que todos los participantes de la red tienen acceso al libro de transacciones, nadie puede alterarlas o cambiarlas, y toda esta información se almacena en la cadena de bloques y se ejecuta automáticamente, mejorando la velocidad en las transacciones (IBM, s. f.).

Las criptomonedas están basadas en la tecnología Blockchain; actualmente, existen varios tipos de criptomonedas, sin embargo, las más conocidas son el Bitcoin y el Ethereum. Estas se administran únicamente a través de carteras digitales que pueden ser una aplicación móvil o de escritorio.

La gran diferencia entre Bitcoin y Ethereum es la forma en que se realiza el minado. En Ethereum, un minero puede cobrar por confirmar la transacción, además de no existir un límite para la emisión de Ethereum, como sí existe en Bitcoin (21 millones) (Plus500, s. f.-a).

**Tabla 2**

*Comparativa entre Bitcoin y Ethereum*

| **Características** | **Bitcoin** | **Ethereum** |
| --- | --- | --- |
| **Creador** | Satoshi Nakamoto | Vitalik Buterin |
| **Financiación** | Sin financiación | ICO en 2014, 18 millones de $ recaudados. |
| **Nivel de descentralización** | Alto | Medio (muchas decisiones dependen de un pequeño grupo de personas) |
| **Precio moneda** | Alto, su precio se consolida por una política deflacionaria, aceptación y confianza. | Medio, su precio fluctúa debido a la emisión inflacionaria y la presión al alza del Bitcoin. |
| **Emisión total de monedas** | Limitada (aprox. 21 millones de monedas) | Ilimitada (la emisión total no está limitada, la emisión anual de momento se mantiene en 18 millones, ETH 2.0 la llevará a 2 millones anuales). |
| **Minería** | Algoritmo de Prueba de Trabajo (PoW) con SHA-256 | Actualmente, algoritmo PoW con Ethash (Keccak); con ETH 2.0, el algoritmo cambiará a Proof of Stake (PoS). |
| **Escalabilidad** | Actualmente, 6-8 transacciones por segundo. Con LN y otros canales de pago, las transacciones son casi instantáneas. | Entre 16-20 transacciones por segundo. Con el cambio a ETH 2.0, se podrá llegar teóricamente hasta las 100.000 transacciones por segundo. |
| ***Smart Contracts*** | Limitado. De momento no hay soporte Turing Completo. | Avanzado. Soporte para Turing Completo y un lenguaje de programación flexible para facilitar la codificación. |

Nota. Adaptada de Bit2me Academy (s. f.).

**Token**

Los *tokens* son la parte esencial de las transacciones digitales, están fundamentados en Blockchain y criptografía, y su función depende del valor que la entidad emisora establezca; sus usos son variados, desde poder ingresar a un juego en línea, hasta el pago por contratar algún trabajo específico.

Unos de los *tokens* más representativos son los NFT o *tokens* no fungibles, los cuales son productos digitales únicos, que no se consumen una vez se usan y no es posible sustituirlos por otros *tokens*. Estos también utilizan la tecnología Blockchain, pero la diferencia entre los *tokens* y las criptomonedas radica en su sustitución; una criptomoneda puede ser sustituida por otra equivalente, los *tokens* no pueden ser sustituidos, por lo que reciben la denominación de “no fungibles”.

La principal diferencia entre un *token* y una criptomoneda es que las criptomonedas utilizan su propia cadena de bloques, mientras que los *tokens* utilizan la cadena de bloques de otra criptomoneda para operar.

**Minado de bloques**

Es un proceso que permite crear nuevos Bitcoins cada vez que alguien los envía o recibe. En este caso, los mineros procesan bloques de transacciones, lo cual es realizado por un sistema de *hardware* especializado (computadores de alta capacidad de procesamiento), mediante resolución de problemas complejos matemáticos.

Un bloque de transacciones o cadena de bloques se va creando cada vez que los mineros descifran el algoritmo matemático y envían su respuesta; esa información se almacena en un bloque para el receptor y la información que este receptor genera también quedará en el récord de la transacción, y así sucesivamente, hasta dar por finalizada la operación, la cual quedará con toda la información generada en cada una de las transacciones realizadas.

Los mineros deben validar que la solución del algoritmo matemático sea correcta, para evitar duplicaciones y lograr una red más segura; por lo tanto, cada nodo de minería Bitcoin rechazará todo aquello que no se ajuste a las normas de los sistemas a minar.

Este proceso de minado debe cumplir tres principios fundamentales para dar cumplimiento a la seguridad de la cadena:

* **El *hash***
* **La capacidad de rechazar transacciones y bloques inválidos**
* **Los protocolos de consenso, descentralización y teoría de juegos**

Conozca estos tres principios fundamentales del minado:



1. ***Trading***

El *trading* en criptoactivos es la acción de tomar posición financiera de venta o de compra al precio de una criptomoneda frente al dólar (Criptomoneda-dólar) o frente a otra criptomoneda (Criptomoneda-Criptomoneda) (Plus500, s. f.-c).



Las criptomonedas se pueden negociar por el método de intercambio digital (comprando-vendiendo en un mercado de intercambio de criptomonedas) o mediante derivados financieros (Contratos por Diferencia CFD), en los que existe menor desembolso de capital y permiten especular en el precio del activo digital.

Existen diversas casas de intercambio en la red facilitando carteras virtuales con las que se puede comprar y vender criptomonedas. El riesgo es que estas carteras pueden ser *hackeadas* y perder todo el dinero invertido. Coinbase y Kraken son carteras digitales que permiten comprar Bitcoin, Ethereum, BitcoinCash o Litecoin.

Por otra parte, si se quiere invertir en criptomonedas alternativas con una valoración menor en el mercado (Altcoins), se deben utilizar Bitcoins o Ethereums y enviarlos a otras plataformas de *trading* de criptoactivos, como Binance o Kucoin, donde se pueden hacer intercambios con Altcoins.

**Aplicaciones**

En los últimos tiempos, desde que se creó el Bitcoin, el *trading* de criptomonedas ha empezado a tomar cada vez más fuerza. 

Estas operaciones se pueden realizar a través de plataformas especializadas, y como el sistema es completamente descentralizado, no existe un banco central que regule su circulación, por lo tanto, en muchos países no son consideradas como una moneda legal.

Los contratos por diferencias CFD permiten especular sobre los precios de las criptomonedas, sin tener que ser el dueño de las criptodivisas; se pueden hacer operaciones de compra o negociar en largo (sube el precio) o vender y negociar en corto (baja el precio).

Estos productos se mueven a través del apalancamiento, lo que supone inversión en grupo para tomar posición en el mercado solo con disponer de una mínima parte de la oferta total. Con este mecanismo, se pueden maximizar las ganancias, pero también las pérdidas.



Otra forma de *trading* son los *spreads,* que hacen referencia a la diferencia entre el precio de compra y venta de las criptodivisas; al igual que en los mercados financieros tradicionales, se abre con una posición en el mercado: posición larga, cuando se opera con el precio de compra, y posición corta, cuando se opera con el precio de venta.

El mercado de las criptomonedas está sujeto a las acciones de oferta y demanda; cada criptomoneda tiene su propio valor y aceptación en el mercado, esto se debe principalmente a sus mejoras en diversas áreas, por ejemplo: avances o innovación en su fase de desarrollo, acuerdos en la aceptación de estas como medios de pago en diferentes empresas, amplio rango de acción en intercambio con otras monedas, entre otras. Todo ello permite que el interés por unas criptomonedas o *tokens* sea más interesante que por otras, por lo tanto, aumentaría la demanda y a su vez el precio.

El *trading* a corto plazo (*spread* corto) se da cuando se compra a un valor y, a las pocas horas, se vende a un valor más alto; mientras que el *trading* a largo plazo (spread largo) está basado en comprar criptomonedas y, después de analizar ciertas variables, se puede predecir que su precio subirá en semanas, meses o años.

1. **Limitaciones y control de Blockchain**

Con el imparable crecimiento de las criptomonedas, se ha convertido en una acción primordial para las entidades gubernamentales desarrollar e implementar leyes que regulen su uso e intercambio de manera segura, evitando prácticas ilegales, como el lavado de activos o estafas a los consumidores.

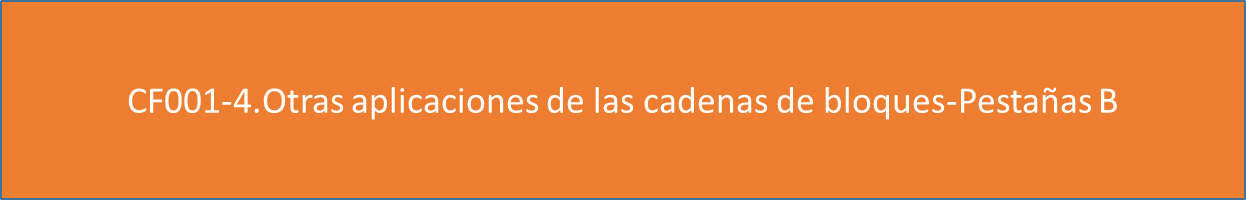
En Colombia, aún no se cuenta con una ley que regule estas prácticas; sin embargo, existe un proyecto de ley que está en curso y pendiente de revisión y aprobación por parte del Congreso de la República, donde se describen todos los pormenores en materia de regulación y limitación de las plataformas que realicen el intercambio de los criptoactivos (Congreso de la República, 2019).

Vea a continuación los avances que se tienen al momento en materia de regulación y control:

| Aunque en Colombia aún no existe una ley que regule las operaciones con criptomonedas y las empresas que se dedican a esta práctica, algunas entidades se han dado a la tarea de emitir algunos conceptos que pueden servir de regulación en el mercado colombiano: | |
| --- | --- |
| Superintendencia Financiera: | |
| Mediante circular 29-2014: aseguró que las monedas virtuales no estaban reguladas por la ley ni estaban sujetas a control o vigilancia por esta entidad. | Mediante circular 52-2017, señala de manera más restrictiva que “no se encuentran autorizadas para custodiar, invertir, intermediar ni operar con estos instrumentos, así como tampoco permitir el uso de sus plataformas para que se realicen operaciones con monedas virtuales”, argumentando la volatilidad e incertidumbre en las operaciones de estos criptoactivos. |
| DIAN: | Superintendencia de Sociedades: |
| Mediante Concepto 20436 del 2017, señala que las actividades asociadas a los criptoactivos están gravadas a través de la renta. | Mediante oficio 100-237890 del 2020, indicó que los criptoactivos pueden ser aceptados como aportes en especie a una sociedad. |
| Consejo Técnico de Contaduría Pública | Banco de la República |
| Publica el Concepto 977 de 2017, donde afirma que “los criptoactivos pueden ser asimilados a *commodities* de inventario o a un activo financiero”. | Mediante Concepto 20348 del 2016, indicó que “los criptoactivos no deben ser considerados como divisas, dado que no cuentan con el respaldo de un Banco Central”. |

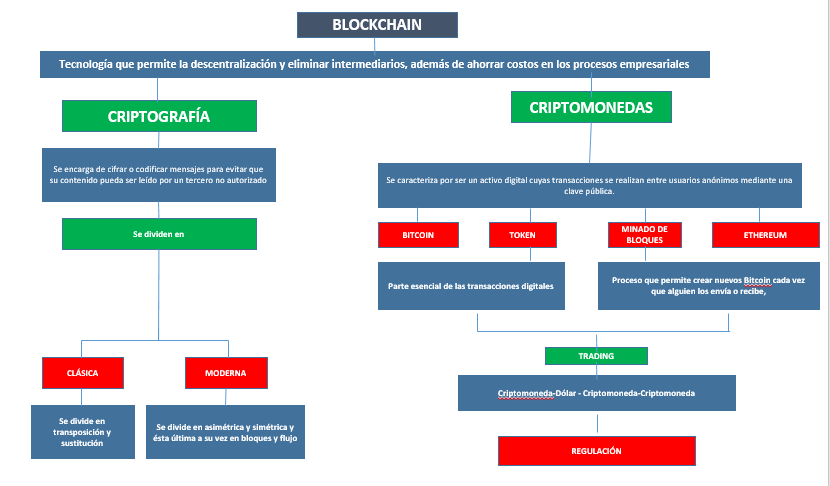
El Blockchain*,* o cadena de bloques, cumple con los criterios de transparencia y confiabilidad, por lo tanto, contiene todo el historial de las transacciones realizadas. Esta tecnología limita el riesgo de fraude, optimiza tareas, aumenta la velocidad de las transacciones, descentraliza las tareas, entre otras; toca esperar avances en legislación y normatividad, pero por lo pronto es una tecnología que llegó para quedarse.

Por último, y como ya se ha visto, además de las criptomonedas y los casos presentados, la tecnología Blockchain es usada con infinidad de aplicaciones y campos de acción; a continuación, se presentan otras aplicaciones actuales que le podrán servir de guía para su aplicación en el campo laboral:



1. **Síntesis**

En el siguiente gráfico, podrá observar una síntesis de los fundamentos del Blockchain y su aplicación en el ámbito financiero:



.

1. **Actividades didácticas**

| DESCRIPCIÓN DE ACTIVIDAD DIDÁCTICA 1 | |
| --- | --- |
| Nombre de la Actividad 1 | El Blockchain y la criptografía |
| Objetivo de la actividad | Facilitar al aprendiz la identificación de conceptos claves de los fundamentos generales de Blockchain y criptografía. |
| Tipo de actividad sugerida | Interfaz de usuario gráfica  Descripción generada automáticamente |
| Archivo de la actividad  (Anexo donde se describe la actividad propuesta) | Anexo\_CF001\_ActividadDidactica1 |

| **DESCRIPCIÓN DE ACTIVIDAD DIDÁCTICA 2** | |
| --- | --- |
| **Nombre de la Actividad 2** | ¿Qué tanto conoces ahora de Blockchain? |
| **Objetivo de la actividad** | Emparejar conceptos relacionados con Blockchain para su apropiación y aplicación en su vida laboral. |
| **Tipo de actividad sugerida** | Interfaz de usuario gráfica  Descripción generada automáticamente |
| **Archivo de la actividad**  **(Anexo donde se describe la actividad propuesta)** | Anexo\_CF001\_ActividadDidactica2 |

1. **Material complementario**

| Tema | Referencia APA del Material | Tipo de material  (Video, capítulo de libro, artículo, otro) | Enlace del Recurso o  Archivo del documento o material |
| --- | --- | --- | --- |
| 1. Blockchain | Espinosa, S. (2020). *Guía de Referencia de Blockchain para la Adopción e Implementación de Proyectos en el Estado Colombiano.* Ministerio de Tecnologías de la Información y las Comunicaciones [MinTIC]. | Guía de Referencia | <https://gobiernodigital.mintic.gov.co/692/articles-161810_pdf.pdf> |
| Rojo, M. (2019). *Blockchain. Fundamentos De La Cadena De Bloques.* Ediciones De La U. | Libro | <https://login.bdigital.sena.edu.co/login?url=http://www.ebooks7-24.com/?il=9093> |
| Böhme, R., Christin, N., Edelman, B. y Moore, T. (2015). Bitcoin: Economics, Technology, and Governance*.* *The Journal of Economic Perspectives, 29*(2), p. 213-238. | Artículo | <https://login.bdigital.sena.edu.co/login?url=https://gateway.proquest.com/openurl?issn=0895-3309&spage=213&url_ver=Z39.88-2004&date=2015-04-01&genre=article&issue=2&res_dat=xri%3Apqm&rft_val_fmt=info%3Aofi%2Ffmt%3Akev%3Amtx%3Aarticle&volume=29&rfr_id=info%3Axri%2Fsid%3Aprimo&jtitle=The%2BJournal%2Bof%2BEconomic%2BPerspectives&req_dat=xri%3Apqil%3Aclntid%3D31491> |
| CEU IAM Business School. (2019). *Blockchain y su aplicación en el ámbito financiero*. [Video]. YouTube. | Video | <https://www.youtube.com/watch?v=lkO168P39Z0&ab_channel=CEUIAMBusinessSchool> |
| 3. Criptomonedas | Congreso de la República de Colombia. (2018). *Proyecto de ley: “Por el cual se regula el uso de las monedas virtuales o criptomonedas y las formas de transacción con éstas en el territorio de Colombia y se dictan otras disposiciones”.* | Proyecto de ley | <http://leyes.senado.gov.co/proyectos/images/documentos/Textos%20Radicados/proyectos%20de%20ley/2018%20-%202019/PL%20028-18%20Criptomonedas.pdf> |
| Gomila, J. (2021) *¿Qué tan complicado es el problema matemático que se resuelve al minar un bloque en Blockchain?* [Video]. YouTube. | Video | <https://www.youtube.com/watch?v=FkHFG-8oNm4&list=RDCMUCMUxXNYrVCv6-bQakhomvBg&index=3> |

1. **Glosario**

| **TÉRMINO** | **SIGNIFICADO** |
| --- | --- |
| **Bitcoin** | Criptomoneda basada en la tecnología Blockchain. Se administra únicamente a través de carteras digitales, que pueden ser una aplicación móvil o de escritorio (Plus500, s. f.-a). |
| **Blockchain** | En español, cadena de bloques, es una tecnología que permite transacciones digitales mediante registros descentralizados, sin ningún tipo de intermediarios (Gupta, 2017). |
| **Criptografía** | Es la disciplina encargada de mantener los datos seguros y que el intercambio de información sea perfectamente confiable. Se basa en el desarrollo de algoritmos cada vez más complejos, por lo tanto, la privacidad es completa (BBVA, 2020). |
| **Criptomonedas** | Aplicación del Blockchain. Activo digital cuyas transacciones se realizan entre usuarios anónimos mediante una clave pública. Todo usuario maneja una clave privada (única por usuario) y una clave pública, que es la que se comparte con los demás usuarios de la red (Dwyer, 2014). |
| **Descentralización** | Realizar transacciones directas, sin ningún tipo de intermediario, disminuyendo costos y aumentando la velocidad (Delgado, 2014). |
| ***Hash*** | Código alfanumérico que se obtiene al aplicar una función matemática a un conjunto de datos concatenados. Contiene toda la información relevante que se quiere encriptar. |
| ***Nonce*** | Código alfanumérico aleatorio que identifica un bloque e introduce seguridad. |
| ***Trading*** | Tomar posición financiera de venta o de compra al precio de una criptomoneda frente al dólar (Plus500, s. f.-c). |

1. **Referencias bibliográficas**

BBVA. (2020). *¿Qué es la criptografía avanzada?* <https://www.bbva.com/es/que-es-la-criptografia-avanzada/>

Bit2me Academy. (s. f.). *Diferencias entre Bitcoin y Ethereum*. <https://academy.bit2me.com/diferencias-entre-bitcoin-y-ethereum/>

Congreso de la República de Colombia. (2018). *Proyecto de ley: “Por el cual se regula el uso de las monedas virtuales o criptomonedas y las formas de transacción con éstas en el territorio de Colombia y se dictan otras disposiciones”.* <http://leyes.senado.gov.co/proyectos/images/documentos/Textos%20Radicados/proyectos%20de%20ley/2018%20-%202019/PL%20028-18%20Criptomonedas.pdf>

Congreso de la República de Colombia. (2019). *Proyecto de Ley 268 de 2019.* *Por la cual se regulan los Servicios de Intercambio de Criptoactivos ofrecidos a través de las Plataformas de Intercambio de Criptoactivos.* Mayo 8 de 2019.

Delgado, I. (2014). *Bitcoin: la moneda virtual descentralizada.* OpenMind BBVA. <https://www.bbvaopenmind.com/economia/finanzas/bitcoin-la-moneda-virtual-descentralizada/>

Dwyer, G. (2014). *The Economics of Bitcoin and Similar Private Digital Currencies*. SSRN. <https://ssrn.com/abstract=2434628>

Eckard, J. (2019). *Almacenamiento para Blockchain y procesamiento moderno de bases de datos distribuidas*. IBM Systems Blog para Latinoamérica. <https://www.ibm.com/blogs/systems/mx-es/2019/02/almacenamiento-para-blockchain-y-procesamiento-moderno-de-bases-de-datos-distribuidas/>

Espinosa, S. (2020). *Guía de Referencia de Blockchain para la Adopción e Implementación de Proyectos en el Estado Colombiano.* Ministerio de Tecnologías de la Información y las Comunicaciones [MinTIC]. <https://gobiernodigital.mintic.gov.co/692/articles-161810_pdf.pdf>

Gupta, V. (2017). *The Promise of Blockchain Is a World Without Middlemen*. Harvard Business Review. <https://hbr.org/2017/03/the-promise-of-blockchain-is-a-world-without-middlemen>

IBM. (s. f.). *¿Qué es la tecnología de Blockchain?* <https://www.ibm.com/co-es/topics/what-is-blockchain>

Medina, L. (2017) *Criptografía y mecanismos de seguridad*. Fundación Universitaria del Área Andina. <https://digitk.areandina.edu.co/bitstream/handle/areandina/1423/Criptograf%C3%ADa%20y%20mecanismos%20de%20seguridad.pdf?sequence=1&isAllowed=y>

Plus500 (s. f.-a). *¿Cuál es la diferencia entre Ethereum y Bitcoin?* <https://www.plus500.com/es-ES/Instruments/ETHUSD/What-is-the-difference-between-Ethereum-and-Bitcoin~2>

Plus500 (s. f.-b). *Halving de Bitcoin 2020: Todo lo que necesita saber.* <https://www.plus500.com/es-ES/Instruments/BTCUSD/Bitcoin-Halving-2020:-All-you-need-to-know~4#:~:text=Un%20Halving%20de%20Bitcoin%20ocurre,lugar%20durante%20mayo%20de%202020>

Plus500 (s. f.-c). *¿Qué es el Trading de Criptomonedas?* <https://www.plus500.com/es-ES/Trading/CryptoCurrencies/What-Is-Cryptocurrency-Trading~3>

Superintendencia de Sociedades. (2020). *Oficio 100-237890 del 14 de diciembre de 2020. Asunto: Criptoactivos – su utilización en actos de comercio – aporte en especie al capital de una sociedad.* <https://www.supersociedades.gov.co/nuestra_entidad/normatividad/normatividad_conceptos_juridicos/OFICIO_100-237890_DE_2020.pdf>

Velasco, J. (2014). *Breve historia de la criptografía*. ElDiario.es. <https://www.eldiario.es/turing/criptografia/breve-historia-criptografia_1_4878763.html>

Wild, J., Arnold, M. y Stafford, P. (2015) *Technology: Banks seek the key to blockchain*. Financial Times. [www.ft.com/content/eb1f8256-7b4b-11e5-a1fe-567b37f80b64?segid=0100320#axzz3qK4rcvqp](http://www.ft.com/content/eb1f8256-7b4b-11e5-a1fe-567b37f80b64?segid=0100320#axzz3qK4rcvqp).

1. **Control del documento**

|  | Nombre | Cargo | Dependencia | Fecha |
| --- | --- | --- | --- | --- |
| Autor(es) | Norma Constanza Morales Cruz | Experta Temática | Regional Tolima - Centro de Comercio y Servicios | Marzo 2022 |
| Abel Fernando Becerra Carrillo | Experto temático | Región Norte de Santander - Centro de la industria, la empresa y los servicios | Marzo 2022 |
| Zvi Daniel Grosman | Diseñador Instruccional | Regional Distrito Capital – Centro de Gestión Industrial | Marzo 2022 |
| Andrés Felipe Velandia Espitia | Asesor Metodológico | Regional Distrito Capital - Centro de Diseño y Metrología | Marzo 2022 |
| Rafael Neftalí Lizcano Reyes | Responsable Equipo  Desarrollo Curricular | Regional Santander - Centro Industrial del Diseño y la Manufactura | Marzo 2022 |
| Darío González | Corrección de estilo | Regional Distrito Capital - Centro de Diseño y Metrología | Marzo 2022 |

1. **Control de cambios**

**(Diligenciar únicamente si realiza ajustes a la Unidad Temática)**

|  | Nombre | Cargo | Dependencia | Fecha | Razón del cambio |
| --- | --- | --- | --- | --- | --- |
| Autor(es) |  |  |  |  |  |