# LA TECNOLOGÍA BLOCKCHAIN Y SU IMPLEMENTACIÓN COMO VALIDADOR DE TRANSACCIONES FINANCIERAS EN EL COMERCIO ELECTRÓNICO DE COLOMBIA

WILLIAM EDISON VANEGAS RODRIGUEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
IBAGUE
2023

# LA TECNOLOGÍA BLOCKCHAIN Y SU IMPLEMENTACIÓN COMO VALIDADOR DE TRANSACCIONES FINANCIERAS EN EL COMERCIO ELECTRÓNICO DE COLOMBIA

WILLIAM EDISON VANEGAS RODRIGUEZ

Proyecto de Grado – Monografía presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Director de trabajo de grado
Ing. MSC Edgar Mauricio López

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
IBAGUE
2023

NOTA DE ACEPTACIÓN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

## DEDICATORIA

Con amor dedico este trabajo a mi padre que ya no se encuentra entre nosotros, a mi madre y hermana que, con su apoyo, hicieron posible la culminación de mi pregrado como ingeniero electrónico.

## AGRADECIMIENTOS

Agradezco a los tutores de la UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD, al personal administrativo, y en especial los pertenecientes a la escuela ECBTI CEAD Ibagué, que siempre estuvieron a disposición para colaborarme en la realización de este documento.

**CONTENIDO**

Pág.

## INDICE DE FIGURAS

## INDICE DE TABLAS

# ANEXOS

## GLOSARIO

**Blockchain:** Es una tecnología de registro distribuido que utiliza una red descentralizada de computadoras (nodos) para almacenar y verificar transacciones de manera segura. Cada transacción se cifra y se agrupa en bloques, y estos bloques se enlazan entre sí de forma cronológica, creando una cadena inmutable de datos. La característica distintiva de una BLOCKCHAIN es su resistencia a la modificación, ya que una vez que se confirma una transacción, es prácticamente imposible alterarla sin el acuerdo de la mayoría de los nodos en la red.
las aplicaciones de BLOCKCHAIN se han diversificado para incluir registros de propiedad, gestión de cadenas de suministro, votaciones electrónicas seguras, autenticación de identidad y más. Su diseño descentralizado y su capacidad para garantizar la confiabilidad y la transparencia la hacen relevante en una amplia variedad de campos.

**Criptomoneda:** Es un activo digital que utiliza un cifrado criptográfico, el cual asegura su integridad y asegura la trazabilidad de sus transacciones. Estas monedas no son físicas, se almacenan en billeteras digitales denominadas wallets.

**Ledger:** Es un libro digital mayor, distribuido en toda la BLOCKCHAIN donde se registran las transacciones que se realizan. Dependiendo de la naturaleza de la BLOCKCHAIN este puede ser público o privado.

**Minería**: En términos informáticos, es el proceso en el que se agregan bloques a una BLOCKCHAIN, utilizando la potencia informática de los nodos.

**NFT:** Se denominan por sus siglas en ingles token no fungible, son piezas únicas que no pueden ser intercambiadas o segmentadas, es el nuevo concepto de subastas de arte, pueden existir diversas copias de una obra, pero solo su dueño es el verdadero poseedor de esta. Se pueden entender como certificados digitales de propiedad.

**Nodo:** Es un sistema informático que sirve para validar transacciones utilizando el poder de procesamiento a nivel de hardware. Por el uso de estos equipos informáticos, los operadores reciben pago o recompensa en criptomonedas que dependerá de la BLOCKCHAIN validada si, por ejemplo, se están validando transacciones de la red Ethereum, las recompensas serán en la criptomoneda ETH[1].

**Peer to Peer:** Es una red de computadores que están interconectados como nodos, trabajan como clientes y servidores al mismo tiempo, estos permiten el intercambio de información, en cualquier formato.

[1] Abreviación de la criptomoneda Ethereum

**Smartcontracts**: Se denominan contratos inteligentes, básicamente es un código que es capaz de ejecutar un contrato a si mismo sin la intervención de terceros, en lugar de utilizar un documento en físico que puede ser susceptible a alteraciones.

**Traders:** Individuos o entidades que se dedican a comprar, vender o intercambiar instrumentos financieros, materias primas u otros activos en diversos mercados. Su objetivo principal es obtener ganancias a partir de las fluctuaciones de precios de estos activos a lo largo del tiempo.

## RESUMEN

En este documento, se abordará cómo la tecnología de la cadena de bloques, o BLOCKCHAIN, debido a su peculiar funcionamiento, puede proporcionar una protección efectiva y validar datos sensibles, como información financiera, documentos privados e incluso secretos industriales. Estos datos están amenazados por posibles ciberataques que podrían llevar a consecuencias delictivas, como estafas, extorsión o robo de información, que pueden afectar tanto a entidades como a individuos.

En el documento se detallará la diferencia fundamental entre una cadena de bloques centralizada y una descentralizada, explorando sus aplicaciones más comunes y el motivo de su funcionamiento. Además, se examinarán otras funcionalidades que esta tecnología ofrece.

Asimismo, se llevará a cabo un análisis de cómo la implementación de la seguridad de esta tecnología en el comercio electrónico, o E-COMMERCE, en Colombia, podría tener un impacto significativo en la reducción de fraudes financieros.



## ABSTRACT

In this document, we will discuss how blockchain technology, due to its unique operation, can effectively protect and validate sensitive data such as financial information, private documents, and even industrial secrets. This data is susceptible to cyberattacks that may lead to criminal consequences, such as fraud, extortion, or information theft, affecting both entities and individuals.

The document will delve into the fundamental difference between a centralized and a decentralized blockchain, exploring their most common applications and the reason for their operation. Furthermore, it will examine other functionalities that this technology offers.

Additionally, an analysis will be conducted on how implementing the security of this technology in e-commerce, in Colombia, could have a significant impact on reducing financial fraud.

# INTRODUCCIÓN

El propósito fundamental de este documento es resaltar cómo la tecnología BLOCKCHAIN ofrece una confianza sólida en el ámbito del comercio electrónico, convirtiéndolo prácticamente en una fortaleza invulnerable frente a potenciales ataques cibernéticos.

La BLOCKCHAIN se ha erigido como una herramienta poderosa para la validación de transacciones de diversa índole, e incluso se están explorando sus posibilidades para mejorar la seguridad en el ámbito de la inteligencia artificial.

Esta tecnología adquirió una relevancia significativa a partir del año 2008, coincidiendo con la introducción de la criptomoneda bitcoin. La creación de esta nueva forma de intercambio de bienes y servicios, atribuida posiblemente a una figura enigmática o a un grupo de programadores conocidos como Satoshi Nakamoto, marcó un hito en la historia financiera y tecnológica.

Además, en el contexto colombiano, el comercio electrónico ha experimentado un crecimiento acelerado, impulsado en gran medida por la pandemia de COVID-19. Sin embargo, este crecimiento también ha revelado una serie de desafíos, tales como retrasos en las transacciones, entregas que no coinciden con los productos solicitados y, lamentablemente, estafas de gran envergadura. Aquí es donde la BLOCKCHAIN emerge como una solución capaz de mitigar estas deficiencias en materia de seguridad informática.

Este documento explorará detalladamente cómo la BLOCKCHAIN puede ofrecer una solución sólida y eficaz para mejorar la seguridad y la confiabilidad en el entorno del comercio electrónico, particularmente en el contexto colombiano, donde la necesidad de soluciones robustas es más evidente que nunca.

# 1 DEFINICIÓN DEL PROBLEMA

En razón a lo expuesto anteriormente, la propuesta busca dar respuesta a la siguiente pregunta:

¿Podría la tecnología BLOCKCHAIN mejorar la seguridad en las transacciones financieras?

## 1.1 ANTECEDENTES DEL PROBLEMA

Según la revista Portafolio, la virtualización, que se incrementó notablemente durante las distintas etapas de confinamiento, tuvo un impacto significativo en la incidencia de delitos informáticos en Colombia[2], en particular en el aumento de los casos de hurto por medios informáticos. En el año 2020, se registró un incremento del 37% en comparación con el año 2019, con un total de 16,654 denuncias presentadas.

Aunque en Colombia estos tipos de delitos ya eran comunes antes de la pandemia de COVID-19, las cuarentenas prolongadas llevaron a una gran cantidad de transacciones virtuales, muchas de las cuales, siendo realistas, no estaban adecuadamente protegidas contra ciberataques. Este contexto creó un ambiente propicio para que los ciberdelincuentes pudieran explotar vulnerabilidades, lo que resultó en pérdidas significativas tanto en términos económicos como en bienes y servicios.

En este escenario, los ciberdelincuentes encontraron oportunidades relativamente fáciles debido al aumento de la virtualidad. Les bastaba con enviar publicidad engañosa que inducía a las víctimas a proporcionar sus claves personales, lo que facilitaba su estafa.

La situación planteada pone de manifiesto la importancia crítica de la ciberseguridad en un entorno cada vez más digitalizado, donde la protección de datos y la conciencia sobre las amenazas cibernéticas se vuelven esenciales para evitar pérdidas y proteger a los individuos y las organizaciones en el espacio virtual.

En este contexto, la BLOCKCHAIN puede desempeñar un papel importante en la lucha contra los delitos informáticos. Es una tecnología que permite registrar transacciones de forma segura y transparente. Esto la hace una herramienta adecuada para proteger los datos personales y las transacciones financieras.

[2] Fuente: PORTAFOLIO, la virtualidad acelero los delitos informáticos {pagina web} {en línea} {consultado el 24 de octubre 2023} disponible en: https://www.portafolio.co/economia/la-virtualidad-acelero-los-delitos-informaticos-550041

## 1.2 FORMULACIÓN DEL PROBLEMA

En razón a lo expuesto anteriormente, la propuesta busca dar respuesta a la siguiente pregunta:

¿De qué manera la tecnología BLOCKCHAIN fortalece la seguridad de las transacciones electrónicas frente a posibles ciberataques?

# 2 JUSTIFICACIÓN

El avance tecnológico ha transformado la forma en que las personas viven y trabajan, pero también ha traído consigo nuevos desafíos, como los ataques cibernéticos. En este contexto, la tecnología BLOCKCHAIN emerge como una solución alentadora para proteger los datos y las transacciones, ofreciendo una mayor seguridad y transparencia en los procesos, lo que ha llevado a un creciente interés en su adopción a nivel global.

En el contexto tecnológico de Colombia, se ha experimentado un rápido avance tecnológico en las últimas décadas, con un crecimiento significativo en la adopción de dispositivos móviles, conexiones a Internet y la digitalización de servicios. Este cambio ha tenido un impacto positivo en la economía del país, pero también ha aumentado la exposición a las amenazas cibernéticas.

Los ataques cibernéticos son cada vez más sofisticados y representan una seria amenaza para la integridad de datos y la seguridad financiera. El Banco de la República de Colombia y otras instituciones gubernamentales han destacado la importancia de abordar estas amenazas y la necesidad de soluciones efectivas.

Por lo tanto, la tecnología BLOCKCHAIN, es una solución prometedora para proteger los datos y las transacciones, gracias a su arquitectura descentralizada y su resistencia a la alteración. El Banco de la República de Colombia y otros entes gubernamentales han reconocido su potencial en informes y declaraciones relacionadas con tecnología y seguridad financiera.

Además de explicar el funcionamiento de la BLOCKCHAIN y analizar sus ventajas y desventajas, este documento tiene como objetivo fundamental crear conciencia sobre la importancia de proteger los datos en un entorno cada vez más digitalizado. La falta de medidas de seguridad es un problema común, como se ha señalado en informes gubernamentales y estudios, lo que hace que los sistemas informáticos sean vulnerables a ciberataques.

Dada la creciente adopción tecnológica y la amenaza constante de ataques cibernéticos, este documento se justifica en la necesidad de proporcionar información precisa respaldada por instituciones como el Banco de la República de Colombia. Además, busca fomentar la conciencia y la adopción de tecnologías como la BLOCKCHAIN para proteger la seguridad de datos y transacciones en Colombia.

# 3 OBJETIVOS

## 3.1 OBJETIVO GENERAL

Demostrar como la tecnología BLOCKCHAIN proporciona un entorno seguro y libre de manipulación para realizar transacciones, promoviendo la confianza y la integridad en diversos contextos, como transacciones financieras y comercio electrónico.

## 3.2 OBJETIVOS ESPECÍFICOS

1. Examinar los diferentes tipos de BLOCKCHAIN y la aplicabilidad para validar transacciones financieras.

2. Comparar los protocolos proof of work y proof of stake, y su método de funcionamiento en la validación de bloques.

3. Explicar mediante casos aplicados exitosos, como el e-commerce respaldado por una BLOCKCHAIN ofrece una alta confiabilidad de transacciones financieras de diferentes activos.

4. Justificar mediante un breve análisis técnico, como las criptomonedas y tokens puede ser utilizados como medio de pago descentralizado, las cuales se aprecian dependiendo de la BLOCKCHAIN a la que pertenecen.

# 4 MARCO REFERENCIAL

## 4.1 MARCO TEÓRICO

La revolución de la tecnología BLOCKCHAIN, es el resultado de un enfoque matemático y tecnológico que ha evolucionado con el tiempo y ha llevado a organizaciones tanto públicas como privadas a replantear y ajustar sus infraestructuras y modelos de negocio. Para comprender mejor este fenómeno, es necesario profundizar en el concepto teórico y sus implicaciones.

Con la tecnología BLOCKCHAIN, se propicia la transparencia pues según Bernard Marr[3], "es un modelo de base de datos distribuida y encriptada que tiene el potencial de resolver muchos problemas relacionados con la confianza y la seguridad *online"*.

Un componente fundamental para comprender cómo funciona la tecnología BLOCKCHAIN es el concepto de "hash". Un "hash" es una función matemática que toma datos de entrada y los convierte en una cadena de caracteres alfanuméricos de longitud fija. Estos hashes se utilizan para garantizar la integridad de los datos en cada bloque de la cadena.

En el contexto de la seguridad, cada bloque en una cadena de bloques está protegido por un "hash" que representa su contenido. Cualquier modificación en el contenido del bloque, como la alteración de datos o transacciones, resultaría en un cambio en el valor hash del bloque. Esto significa que, si alguien intenta atacar un bloque o una secuencia de bloques, la red detectaría inmediatamente la discrepancia entre los valores hash y rechazaría la transacción fraudulentamente, manteniendo la integridad de la cadena de bloques.

Cada transacción registrada en la cadena es accesible públicamente y se puede verificar en tiempo real. Esto promueve la confianza, ya que las transacciones son visibles y rastreables, lo que disminuye la necesidad de depender de intermediarios y reduce la posibilidad de fraude.

Algunas aplicaciones prácticas:

Criptomonedas: La BLOCKCHAIN, es más conocida por su papel en las criptomonedas como Bitcoin, donde proporciona un registro seguro y transparente de todas las transacciones financieras. Esto ha revolucionado la forma en que se realizan las transacciones y se almacena el valor.

---

[3] Fuente: MARR Bernard, Estas son las cinco mayores tendencias de blockchain para 2022 revista Forbes {Pagina web} {en línea} {consultado el 24 de julio 2023} disponible en https://forbes.es/criptomonedas/126653/estas-son-las-cinco-mayores-tendencias-de-blockchain-en-2022/

Gestión de la Cadena de Suministro: Se utiliza para rastrear productos desde su origen hasta su destino final, proporcionando visibilidad y autenticidad en cada paso del proceso.

Registros de Propiedad: Se ha implementado esta tecnología para mantener registros inmutables de la propiedad de activos, lo que reduce la posibilidad de litigios y fraudes.

Votación Electrónica Segura: Una BLOCKCHAIN, puede garantizar elecciones seguras y transparentes al proporcionar un registro inmutable de votos.

Descentralización y Seguridad: La estructura descentralizada de la BLOCKCHAIN significa que no depende de una entidad central de confianza. En lugar de eso, se basa en el consenso de múltiples nodos en la red para validar y registrar transacciones. Esto la hace altamente segura y resistente a la alteración.

La capacidad de una BLOCKCHAIN para proporcionar transparencia y seguridad en línea ha llevado a su adopción en diversas aplicaciones, y su impacto en organizaciones públicas y privadas continúa expandiéndose a medida que se exploran nuevas oportunidades en el mundo digital. En resumen, la tecnología BLOCKCHAIN ofrece un nivel avanzado de seguridad y transparencia que puede resistir intentos de alteración y ataques, lo que la hace una herramienta poderosa para muchas aplicaciones en la actualidad.

## 4.2 MARCO CONCEPTUAL

Para comprender el funcionamiento general de una BLOCKCHAIN, es necesario explorar sus componentes y procesos en detalle. A continuación, se describirán los elementos clave de su funcionamiento tener en cuenta los siguientes conceptos[4]:

**Criptografía asimétrica**: también se denomina encriptación de clave publica, es un método que utiliza dos claves para el envío de mensajes, una de ellas es pública y la otra es privada, es decir, solo el usuario la conoce.

Este método criptográfico, garantiza que este par de claves solo se puede generar una vez haciéndola única, no es posible que dos usuarios tengan el mismo juego de claves.

**Redes Peer to Peer:** También denominadas colega a colega, son aquellas redes que permiten a los usuarios conectarse entre sí y compartir archivos que se

[4] Fuente: IONOS Digital Guide, blockchain {Pagina web} {en línea} {consultado el 21 de octubre de 2023} disponible en: https://www.ionos.es/digitalguide/online-marketing/vender-en-internet/blockchain/

encuentran en sus equipos de cómputo, todos los días utilizamos este tipo de redes casi involuntariamente.

**Algoritmos de comprobación o de consenso:** Es el mecanismo utilizado por una BLOCKCHAIN para autenticar una transacción y actualizar el libro o base de datos transaccional la cual puede ser pública o privada dependiendo del tipo de BLOCKCHAIN. El consenso se da cuando los nodos validadores peer to peer, están de acuerdo con la transacción. Cualquier cambio de estado llega con el resultado de un cálculo matemático muy complejo que requiere bastante poder de procesamiento.

**Hash:** Es una función matemática que toma datos de entrada y los convierte en una cadena de caracteres alfanuméricos de longitud fija. Los hashes se utilizan en la BLOCKCHAIN para representar y verificar la integridad de los datos en cada bloque. Cualquier cambio en los datos de un bloque, incluyendo transacciones, modificaría el valor del hash, lo que hace que sea extremadamente difícil alterar la información sin ser detectado.

**Bloque:** Es una unidad de datos que almacena un conjunto de transacciones en la cadena de bloques. Cada bloque contiene un sello de tiempo y un valor hash que lo conecta al bloque anterior, creando una secuencia inmutable de bloques.

**Contratos Inteligentes:** Son programas informáticos autónomos que se ejecutan en la BLOCKCHAIN cuando se cumplen ciertas condiciones predefinidas. Estos contratos permiten la automatización de acuerdos y transacciones sin necesidad de intermediarios.

**Minería:** La minería es el proceso mediante el cual los nodos en la red compiten para resolver complejos problemas matemáticos y agregar nuevos bloques a la cadena de bloques. Este proceso se utiliza para garantizar la seguridad y la integridad de la BLOCKCHAIN.

**Nodo**: Es un punto de acceso a la red de BLOCKCHAIN que valida y almacena transacciones, mantiene una copia de la cadena de bloques y participa en la creación de consenso. Los nodos pueden ser operados por individuos o entidades y son esenciales para el funcionamiento de la red.

Estos conceptos son fundamentales para comprender cómo funciona la tecnología BLOCKCHAIN y cómo reacciona frente a posibles ataques o intentos de alteración.

La combinación de criptografía, redes P2P, algoritmos de consenso y otros elementos asegura la integridad y la seguridad de la BLOCKCHIAN, lo que la convierte en una herramienta poderosa para una variedad de aplicaciones.

## 4.3 MARCO HISTÓRICO

Si se busca rastrear el origen de la BLOCKCHAIN tal como se conoce en la actualidad, es necesario remontarse al año 1991. En ese período, la concepción inicial de esta tecnología surgió de la mente de dos distinguidos doctores, Stuart Haber y W. Scott Stornetta[5]. Ambos visionarios compartieron la idea de desarrollar una cadena de bloques codificada y protegida mediante técnicas criptográficas avanzadas, con el propósito de asegurar que ninguna entidad tercera tuviera la capacidad de manipular las marcas de tiempo asociadas a archivos.

La visión de Haber y Stornetta sentó las bases de lo que se convertiría en una de las innovaciones tecnológicas más significativas del siglo XXI. Su concepto de una cadena de bloques, con transacciones organizadas en bloques interconectados, y la aplicación de criptografía para garantizar la seguridad y la integridad de los registros, allanó el camino para una tecnología que cambiaría la forma en que se gestionan los datos, las transacciones financieras y la seguridad en línea.

Posteriormente en 1992, actualizaron el sistema incorporándole arboles de Merkle[6] dando posibilidades de compilar una mayor cantidad de documentos en un solo bloque.

En 2008 este trabajo empieza a ganar importancia gracias al desarrollador o equipo de trabajo con seudónimo Satoshi Nakamoto quien creo el primer BLOCKCHAIN, desde donde la tecnología ha evolucionado de tal manera que hoy en día tiene múltiples aplicaciones como en el caso de estudio que es validador de transacciones financieras.

No obstante, la BLOCKCHAIN tal como se conoce hoy en día no se materializó completamente hasta años más tarde. En 2008, una figura enigmática conocida como Satoshi Nakamoto presentó un documento que describía un sistema de efectivo electrónico peer-to-peer basado en una cadena de bloques, que finalmente daría origen a la criptomoneda Bitcoin. Si bien Nakamoto no fue el inventor original de la BLOCKCHAIN, su contribución fue fundamental para su desarrollo y popularización, ya que puso en práctica los conceptos teóricos previamente establecidos por Haber y Stornetta.

---

[5] Fuente: MALDONADO José, ¿Quién es W Scott Stornetta? Bit2me Academia {página web} {en línea} {consultado el 24 de julio 2023} disponible en: https://academy.bit2me.com/quien-es-w-scott-stornetta/

[6] Fuente: MUÑOZ Aitor, Sistema de Verificación de documentos usando arboles de Merkle,{en línea} Grado de ingeniería informática, Madrid España, Universidad Autónoma de Madrid, Escuela politécnica superior 2018 51p{consultado el 24 de julio 2023}.Disponible en: https://repositorio.uam.es/bitstream/handle/10486/688980/mu%c3%b1oz_cu%c3%b1a_aitor_tfg.pdf?sequence=1&isAllowed=y

La visión de Nakamoto, junto con los principios fundamentales establecidos por Haber y Stornetta, allanaron el camino para la creación de una tecnología revolucionaria que ha transformado la gestión de datos, las transacciones financieras y la seguridad en línea en todo el mundo

La BLOCKCHAIN básicamente es un libro de registro que se distribuye punto a punto muy seguro que su contenido solo puede ser modificado vinculando otro bloque encadenado al anterior.

Se debe tener en cuenta que, BLOCKCHAIN y bitcoin son dos conceptos diferentes, ya que la primera es la tecnología que impulsa diversas aplicaciones entre ellas la criptomoneda del mismo nombre.

Satoshi Nakamoto[7], creo el primer bloque de bitcoin denominado Genesis, desde donde se encadenaron otros bloques dando como resultado una gran cadena que transporta información y transacciones también dio origen al primer bitcoin por lo que esta versión se denomina BLOCKCHAIN 1.0.

Aquí nace también el termino minería criptográfica que es básicamente el uso de computadores los cuales validan las transacciones descifrando el algoritmo de encriptación por medio de su fuerza de procesamiento.

A partir del año 2013, la tecnología BLOCKCHAIN experimentó una evolución significativa hacia lo que se conoce como BLOCKCHAIN 2.0, marcada por la introducción del concepto de 'smart contracts' o contratos inteligentes. Esta innovación fue impulsada en gran medida por la colaboración de Vitalik Buterin, una figura destacada en la comunidad de Bitcoin en ese momento.

Buterin dio un paso audaz al crear su propia BLOCKCHAIN, denominada Ethereum[8], la cual se diferencia de Bitcoin en varios aspectos fundamentales. A diferencia de Bitcoin, que se centra en la transferencia de valor en forma de criptomoneda, Ethereum es una plataforma completamente pública que permite a las personas registrar y ejecutar contratos inteligentes. Estos contratos inteligentes son programas autónomos que operan en la cadena de bloques y pueden automatizar acuerdos, procesos y transacciones.

Ethereum también tiene su propia criptomoneda, denominada Ether (ETH), que es utilizada para pagar tarifas por la ejecución de contratos inteligentes y transacciones en la red. Esta combinación de una plataforma pública, contratos inteligentes y su propia criptomoneda ha convertido a Ethereum en un actor importante en el mundo

[7]Fuente: NAKAMOTO, Satoshi. [2008]. Bitcoin: A Peer-to-Peer Electronic Cash System. Recuperado de https://bitcoin.org/bitcoin.pdf

[8] Fuente: Buterin, V. (2023). Ethereum Whitepaper Platform https://ethereum.org/en/whitepaper

de la tecnología BLOCKCHAIN y ha permitido una amplia gama de aplicaciones más allá de las transacciones financieras tradicionales

En la figura 1, se puede evidenciar que la valoración de la criptomoneda ETH desde el año 2017 ha sido ascendente, también en la figura 2 se puede ver la capitalización en dólares (USD) de mercado de diversas criptomonedas pertenecientes a varios tipos de BLOCKCHAIN teniendo como principal el bitcoin cuya valoración también ha venido en aumento.

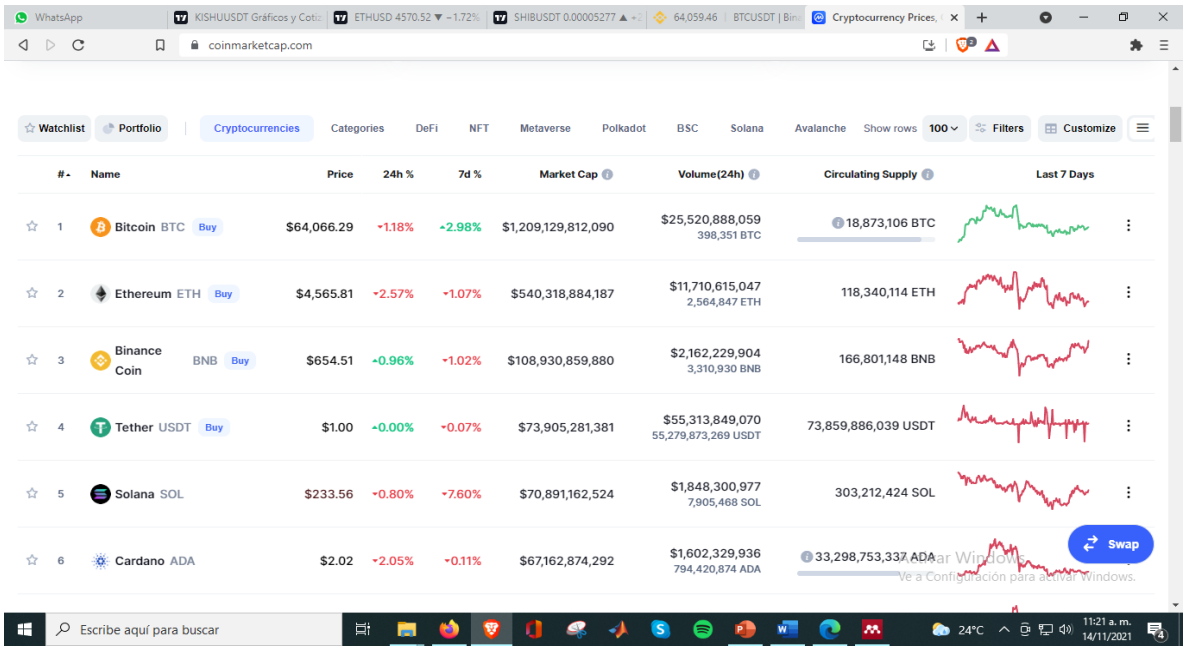
**Figura 1 Capitalización de Ethereum (ETH) desde 2017**


Fuente: https://es.tradingview.com/chart/BXhuHDwr/?symbol=KRAKEN%3AETHUSD

TradingView[9] es una plataforma en línea que ofrece herramientas de análisis técnico y gráficos para traders e inversores. La plataforma cuenta con una amplia variedad de herramientas para análisis de mercados financieros, incluyendo gráficos avanzados, indicadores técnicos, herramientas de dibujo, noticias y análisis fundamentales, entre otros. La plataforma es muy popular entre los traders y analistas técnicos de todo el mundo.

[9] Fuente: TRADINGVIEW Eth/USD/1M {página web} {en línea} {consultado el 1 de noviembre 2021} disponible en: https://es.tradingview.com/chart/BXhuHDwr/?symbol=KRAKEN%3AETHUSD

**Figura 2 Capitalización de mercado de ETH y BTC**




Fuente: **https://coinmarketcap.com/**

CoinMarketCap[10] es un sitio web que ofrece información sobre criptomonedas y activos digitales, incluyendo precios, capitalización de mercado, volumen de operaciones y otra información relevante sobre miles de criptomonedas y tokens. La plataforma es una de las más populares y utilizadas por inversores y traders en todo el mundo para hacer seguimiento de los mercados de criptomonedas.

En el año 2018, la BLOCKCHAIN evoluciona con múltiples proyectos en lo que se denomina BLOCKCHAIN 3.0, como el proyecto NEO el cual se anuncia como primera plataforma BLOCKCHAIN de código abierto, descentralizada. Fue lanzada en China, se denomina el Ethereum Chino.

Aprovechando la funcionabilidad de la BLOCKCHAIN, otros desarrolladores crearon IOTA, está orientada al ecosistema del internet de las cosas (IOT), aborda tarifas de transacción propias y soluciona algunos problemas de escalabilidad de la red BTC 1.0[11]

También se crearon otras BLOCKCHAIN como Monero Zcash las cuales están orientadas a abordar problemas de escalabilidad y seguridad con las primeras aplicaciones BLOCKCHAIN.

[10] Fuente: COINMARKETCAP Capitalización {página web} {en línea} {consultado el 14 de noviembre 2021} disponible en: https://coinmarketcap.com/
[11] Abreviación de la criptomoneda Bitcoin

En 2015 la BLOCKCHAIN evoluciona al concepto denominado Hyperledger[12], fue creado por la fundación Linux. Tiene como particularidad que es de código abierto, su enfoque es el fomento de la tecnología BLOCKCHAIN para mejorar el rendimiento y confiabilidad de los sistemas actuales para respaldar transacciones a nivel global.

En 2017 la compañía privada block.one crea un nuevo protocolo de BLOCKCHAIN impulsado por la criptomoneda EOS, la cual pretende emular atributos de computadoras físicas como CPU y GPU. Tiene como objetivo principal el fomento de aplicaciones descentralizadas a través de una compañía autónoma.

Lo que se espera hoy en día con la tecnología BLOCKCHAIN, es bastante prometedor, incluso gobiernos están invirtiendo capital en búsqueda de innovación y aplicaciones.

Hace poco el gobierno de El Salvador, aprobó el BTC como moneda de curso legal, es posible comprar bienes y servicios, e incluso la persona que posea 3 BTC se le puede otorgar nacionalidad.

## 4.4 ANTECEDENTES O ESTADO ACTUAL

En la última década, la tecnología BLOCKCHAIN ha sido ampliamente reconocida por su capacidad para garantizar la seguridad, la transparencia y la descentralización en diversos sectores, particularmente en el ámbito de las criptomonedas. Sin embargo, su versatilidad ha llevado a investigadores y desarrolladores a explorar nuevas formas de integrar esta tecnología con otros campos innovadores. Uno de los cruces más prometedores se encuentra en la convergencia entre BLOCKCHAIN e Inteligencia Artificial (IA). Este matrimonio tecnológico ha dado lugar a soluciones revolucionarias en áreas tan diversas como la robótica y la sostenibilidad energética. Algunas aplicaciones en las que la tecnología BLOCKCHAIN está siendo implementada:

**La Fusión de BLOCKCHAIN e Inteligencia Artificial[13]:** La robótica ha experimentado un crecimiento exponencial en los últimos años, desempeñando un papel crucial en la automatización industrial, el transporte, la atención médica y muchos otros campos. Sin embargo, a medida que la robótica avanza, también surgen preocupaciones sobre la seguridad y la fiabilidad de estas máquinas altamente complejas. Aquí es donde entra en juego la tecnología BLOCKCHAIN

[12] Fuente: HYPERLEDGER FOUNDATION A Blockchain Platform for the Enterprise {Sitio web} {Consultado el 25 de mayo 2023} Disponible en: https://hyperledger-fabric.readthedocs.io/en/release-2.5/

[13] Fuente: IBM Blockchain e inteligencia artificial (IA) {Sitio web} {Consultado el 21 de octubre de 2023} Disponible en: https://www.ibm.com/mx-es/topics/blockchain-ai

La combinación de BLOCKCHAIN e IA permite establecer un sistema de registro inmutable para el comportamiento y el rendimiento de los robots. Cada acción realizada por un robot se registra en bloques conectados de manera secuencial, lo que crea una cadena de eventos inalterable. Esto brinda a los ingenieros y usuarios la capacidad de rastrear y auditar cada movimiento de los robots, lo que resulta fundamental para identificar y prevenir posibles fallos o accidentes.

Además, esta combinación también habilita la creación de contratos inteligentes específicos para la robótica. Estos contratos pueden establecer reglas y condiciones para el funcionamiento de los robots, asegurando que solo realicen tareas dentro de parámetros seguros y predefinidos. En caso de detectar alguna anomalía o incumplimiento, el contrato inteligente podría detener automáticamente la operación, evitando potenciales daños.

**Energía Sostenible para Nodos Validadores[14]:**

Una de las críticas frecuentes hacia BLOCKCHAIN ha sido la alta demanda de energía que implica la operación de los nodos validadores, especialmente en redes públicas y descentralizadas. El consumo energético significativo está asociado con la resolución de complejos algoritmos matemáticos requeridos para validar transacciones y asegurar la integridad de la red.

Sin embargo, se han realizado avances importantes para abordar este problema y hacer que la minería de criptomonedas sea más sostenible. Una de las soluciones innovadoras ha sido el aprovechamiento de fuentes de energía renovable y respetuosas con el medio ambiente, como la energía volcánica.

En diversas regiones del mundo, especialmente en zonas volcánicas activas, se ha observado una importante liberación de energía geotérmica, proveniente del calor generado por la actividad volcánica. Esta energía geotérmica se puede aprovechar mediante plantas de energía especializadas para producir electricidad.

Empresas mineras de criptomonedas, conscientes de la necesidad de abordar la cuestión de sostenibilidad, han encontrado en la energía volcánica una alternativa prometedora para alimentar sus operaciones. La energía geotérmica proporciona una fuente de electricidad prácticamente inagotable y altamente confiable, ya que no está sujeta a factores climáticos como la luz solar o el viento.

La sinergia entre BLOCKCHAIN e Inteligencia Artificial está revolucionando la robótica, ofreciendo niveles inéditos de seguridad y confianza en la automatización

[14] Fuente: COINTELEGRAPH, Panajachel, Guatemala la minería de bitcoin tiene una nueva sede con energía volcánica en Latinoamérica {Pagina web} {en línea} {Consultado el 21 de octubre de 2023} Disponible en: https://es.cointelegraph.com/news/panajachel-bitcoin-mining-has-new-volcanic-powered-hq-in-latin-america

industrial y otros campos. Los contratos inteligentes basados en BLOCKCHAIN permiten una gestión más segura de los robots, evitando accidentes y mejorando la productividad.

Asimismo, el aprovechamiento de fuentes de energía sostenible, como la energía volcánica, para alimentar los nodos validadores de BLOCKCHAIN es un paso importante hacia la reducción del impacto ambiental de la tecnología de criptomonedas.

**Validación de Transacciones Financieras y su Potencial Mejora en Colombia[15]:**

La validación de transacciones financieras a través de tecnologías como BLOCKCHAIN tiene el potencial de transformar el sistema financiero y mejorar significativamente diversos aspectos en el contexto de Colombia. A continuación, se explorará, cómo la aplicación de esta tecnología en el país puede impulsar la eficiencia, seguridad y transparencia en el sistema financiero local.

En la actualidad, las transacciones financieras en Colombia pueden experimentar demoras significativas, especialmente cuando involucran pagos y transferencias internacionales. Al implementar la tecnología BLOCKCHAIN para la validación de estas transacciones, se podría eliminar la necesidad de intermediarios, reduciendo el tiempo de liquidación y eliminando las barreras impuestas por diferentes sistemas bancarios.

La capacidad de realizar pagos y transferencias de manera casi instantánea, las 24 horas del día y los 7 días de la semana, mejoraría la eficiencia y competitividad del sistema financiero en Colombia, atrayendo más inversionistas y facilitando el comercio tanto a nivel nacional como internacional.

En conjunto, estas innovaciones en BLOCKCHAIN e IA no solo están impulsando la evolución tecnológica, sino que también están allanando el camino hacia un futuro más seguro y sostenible. La combinación de estas tecnologías continúa abriendo puertas a nuevas posibilidades y oportunidades para la sociedad.

Uno de los desafíos clave en Colombia es la falta de acceso a servicios financieros para un gran número de la población, especialmente en áreas rurales y comunidades desfavorecidas. La implementación de BLOCKCHAIN podría impulsar la inclusión financiera al reducir los costos operativos para las instituciones financieras y permitir la creación de soluciones innovadoras para llegar a segmentos de la población no atendidos.

---

[15] Fuente: SIC, La revolución de la confianza digital {Pagina web} {en línea} {Consultado el 21 de octubre de 2023} Disponible en: https://www.sic.gov.co/sites/default/files/files/Propiedad%20Industrial/Boletines_Tecnologicos/Boletin_Blockchain.pdf

## 4.5 MARCO CIENTÍFICO O TECNOLÓGICO

Se debe tener en cuenta, que una parte muy importante de una BLOCKCHAIN son los nodos validadores, pero no todos los nodos participan en resolver el algoritmo o problema matemático del bloque.

Los nodos que si lo hacen son los denominados “mineros” los cuales en el caso de la red bitcoin, utilizan la fuerza de procesamiento de muchos equipos de cómputo interconectados para desencriptar dicho bloque, y el nodo que tenga más poder de procesamiento, será el primero en recibir la recompensa que en este caso será una criptomoneda BTC.

Lo que convierte a una BLOCKCHAIN la opción ideal como validadores de transacciones financieras es que, si un ciberdelincuente va a atacarla, tiene que cambiar todos los bloques de la cadena a partir de que inicio su hackeo, modificando los demás bloques siguientes, lo que ocasionaría que los nodos validadores rechacen los bloques modificados, haciéndola casi invulnerable por los altos costos y recursos que el delincuente necesitaría para robar activos.

Los validadores de la red Bitcoin son responsables de verificar las transacciones y agregarlas a la cadena de bloques. También son responsables de proteger la red de ataques. Los validadores son recompensados por sus servicios con las comisiones por las transacciones. Esta recompensa ayuda a incentivar a los validadores a mantener la red segura y confiable.

Para convertirse en validador, es necesario tener una conexión a Internet de banda ancha y una tarjeta gráfica potente. Las tarjetas gráficas son necesarias para resolver los complejos problemas matemáticos que se utilizan para validar las transacciones y agregarlas a la cadena de bloques. Las tarjetas gráficas son muy caras, por lo que la minería de Bitcoin puede ser una actividad costosa. Sin embargo, también puede ser muy rentable, si se tiene la suerte de encontrar bloques de Bitcoin.

La minería de Bitcoin es una actividad que requiere mucha energía y recursos. Esto ha llevado a preocupaciones sobre el impacto ambiental de la minería de Bitcoin. Algunas personas creen que la minería de Bitcoin debería ser regulada para reducir su impacto ambiental.

A pesar de sus retos ambientales, la minería de Bitcoin también tiene el potencial de ser una actividad beneficiosa para la sociedad. Por ejemplo, la minería de Bitcoin podría ayudar a reducir la dependencia de los sistemas financieros tradicionales, que a menudo son controlados por unos pocos actores. Además, la minería de

Bitcoin podría ayudar a promover la innovación tecnológica, ya que requiere el desarrollo de nuevos métodos de procesamiento de datos.

En última instancia, el impacto ambiental y social de la minería de Bitcoin es un tema complejo que requiere un debate abierto y honesto. Es importante considerar todos los pros y los contras de la minería de Bitcoin antes de tomar una decisión sobre su futuro.

## 4.6 MARCO LEGAL

Actualmente el intercambio de bienes y servicios se materializa a través del dinero emitido por los Estados soberanos, con fundamento el patrón fiduciario y en la soberanía monetaria[16].

Este dinero se denomina FIAT, el cual se conoce como papel moneda que en el caso de Colombia es el peso el cual estuvo respaldado en oro antes de 1993.

Las criptomonedas pretenden cumplir con la misma función del dinero FIAT, servir como medio de pago por bienes y servicios, la gran critica que se ha generado hacia ellas es que son altamente volátiles y no son tangibles como si lo es el dinero, además que no tienen ningún respaldo bancario ni gubernamental.
En Colombia, como en la mayoría de los países no existe una prohibición legal expresa relativa a la utilización de las criptomonedas.

Sin embargo, la DIAN (Dirección de Impuestos y Aduanas Nacionales), ratifico en el concepto 20436 del 2 de agosto de 2017, reiterado por el concepto 000314 del 7 Marzo de 2018, respondió una consulta que tenía como fin aclarar si la minería de criptoactivos estaba gravada o no con el impuesto de renta, en donde la entidad respondió que las criptomonedas no son moneda legal en Colombia, se deduce que la naturaleza jurídica de dichos bienes es la de un bien incorporal susceptible de ser valorado, de conformidad con la definición contenida en el artículo 664 del código civil[17]

[16] Fuente: AYALA ARISTIZABAL, Álvaro. Naturaleza jurídica de las criptomonedas a la luz de los pronunciamientos de soft law en Colombia. Revista Jurídica Piélagus, 2021 20(1), 19. disponible en: https://doi.org/10.25054/16576799.2822

[17] Fuente: DIAN Compilación de la doctrina tributaria vigente relevante en materia de criptoactivos {14 Octubre 2022} {en línea} disponible en:https://www.dian.gov.co/normatividad/Documents/Compilacion-de-la-doctrina-tributaria-vigente-relevante-en-materia-de-criptoactivos.pdf

# 5 DISEÑO METODOLÓGICO

El diseño metodológico propuesto es una investigación exploratoria que tiene como objetivo revisar los conceptos más importantes de la tecnología BLOCKCHAIN a nivel mundial y compararlos con su aplicación en Colombia. Además, se tomarán en cuenta casos exitosos de aplicabilidad y cómo la valoración de algunas criptomonedas ha aumentado a medida que la BLOCKCHAIN a la que pertenecen mejora en términos de seguridad y aplicabilidad.

**Pasos por seguir en la investigación exploratoria**:

**Revisión bibliográfica y documental**: Se recopilarán y analizarán diversas fuentes de información, como artículos científicos, libros, informes técnicos y noticias relacionadas con BLOCKCHAIN y criptomonedas. Se buscará comprender los conceptos clave, la evolución histórica y las tendencias actuales de esta tecnología a nivel global.

**Análisis comparativo con el contexto colombiano**: Se realizará una comparación entre la aplicación de BLOCKCHAIN a nivel mundial y su adopción en Colombia. Se examinarán proyectos y casos prácticos donde la tecnología haya sido utilizada exitosamente en el país, así como las barreras y desafíos específicos que puedan existir en el contexto local.

**Estudio de casos exitosos:** Se identificarán y analizarán casos reales en los que BLOCKCHAIN haya demostrado ser exitoso en distintas industrias o sectores en Colombia. Esto permitirá comprender cómo se ha aplicado con éxito la tecnología en el país y qué beneficios ha aportado.

**Análisis de la relación entre seguridad y aplicabilidad**: Se investigará cómo la mejora de los índices de seguridad y aplicabilidad de una BLOCKCHAIN se ha traducido en un aumento en la valoración de ciertas criptomonedas. Se examinarán los factores que influyen en la confianza de los usuarios y los inversores en estas tecnologías.

**Creación de hipótesis para la implementación en E-COMMERCE colombiano**: A partir de la información recopilada y analizada, se desarrollará una hipótesis sobre los posibles efectos y beneficios que podría tener la implementación más frecuente de BLOCKCHAIN en el E-COMMERCE (comercio electrónico) colombiano. Se plantearán escenarios y se realizarán proyecciones basadas en los resultados obtenidos.

**Comunicación en un lenguaje accesible:** Finalmente, los hallazgos y la hipótesis se presentarán de manera clara y comprensible, utilizando un lenguaje sencillo y

accesible para que cualquier persona interesada en el tema pueda entender los resultados de la investigación.

Es importante destacar que la metodología exploratoria es adecuada para adentrarse en un tema complejo y novedoso como BLOCKCHAIN, ya que permite explorar y comprender sus fundamentos y aplicaciones de manera más amplia y facilita la generación de nuevas ideas y enfoques sobre su potencial implementación en el E-COMMERCE colombiano.

# 6 DESARROLLO DE LOS OBJETIVOS

## 6.1 EXAMINAR LOS DIFERENTES TIPOS DE BLOCKCHAIN Y LA APLICABILIDAD PARA VALIDAR TRANSACCIONES FINANCIERAS

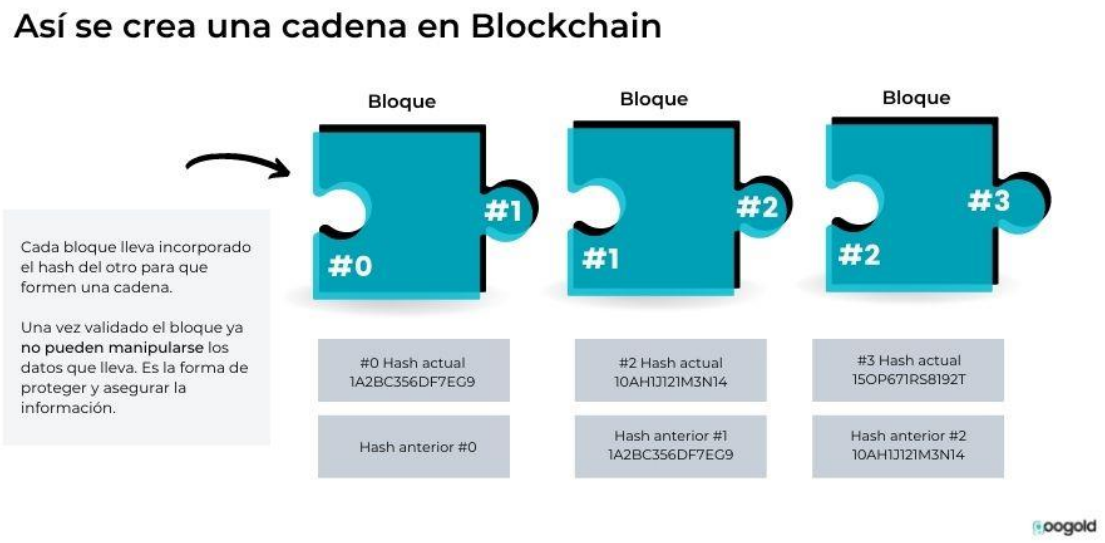
En la actualidad, existen varios tipos de BLOCKCHAIN con características y aplicaciones específicas. La selección del tipo de BLOCKCHAIN más adecuado para validar transacciones financieras en el comercio electrónico es un aspecto crucial que debe considerarse cuidadosamente. En este capítulo, se explorarán los diferentes tipos de BLOCKCHAIN y se analizará cuál sería el más recomendado para este fin.

La figura 3 muestra una BLOCKCHAIN con tres bloques. El primer bloque es el bloque “génesis”, que es el bloque inicial de la cadena. Los bloques siguientes se van añadiendo a la cadena de forma secuencial.

Cada bloque contiene los siguientes datos:

- Hash del bloque anterior: Este hash se utiliza para conectar los bloques entre sí.
- Datos de la transacción: Estos datos incluyen la fecha y la hora de la transacción, el valor de la transacción y las direcciones de los participantes.
- Hash del bloque: Este hash se calcula utilizando los datos del bloque.

**Figura 3: Creación de una cadena de bloques.**




Fuente: https://www.googold.es/aprender-mas/que-es-blockchain-y-por-que-ha-revolucionado-el-sector-financiero/

En el ejemplo de la figura 3, el bloque génesis contiene los siguientes datos:

- Hash del bloque anterior: Este campo está vacío, ya que el bloque génesis es el bloque inicial de la cadena.
- Datos de la transacción: Esta transacción representa la creación de la moneda virtual o criptomoneda.
- Hash del bloque: Este hash se calcula utilizando los datos del bloque génesis.

El bloque 1 contiene los siguientes datos:

- Hash del bloque anterior: Este hash es el hash del bloque génesis.
- Datos de la transacción: Esta transacción representa una transferencia de monedas virtuales de una dirección a otra.
- Hash del bloque: Este hash se calcula utilizando los datos del bloque 1.

El bloque 2 contiene los siguientes datos:

- Hash del bloque anterior: Este hash es el hash del bloque 1.
- Datos de la transacción: Esta transacción representa una transferencia de monedas virtuales de una dirección a otra.
- Datos de la transacción: Esta transacción representa una transferencia de monedas virtuales de una dirección a otra.

En caso de ataque, un atacante podría intentar modificar el bloque 1. Sin embargo, esto sería muy difícil, ya que el hash del bloque cambiaría. Además, los nodos de la red rechazarían el bloque modificado, ya que no sería válido.

Por ejemplo, el atacante podría intentar cambiar el valor de la transacción en el bloque 1. Esto cambiaría el hash del bloque 1, lo que alertaría a la red de que el bloque ha sido modificado. Los nodos de la red rechazarían el bloque modificado, ya que no sería válido.

Otro ataque posible sería intentar añadir un bloque falso a la cadena. Sin embargo, esto también sería muy difícil, ya que los nodos de la red tendrían que aceptar el bloque falso. Esto es poco probable, ya que los nodos de la red están motivados para mantener la integridad de la BLOCKCHAIN.

Cabe resaltar que, los ataques a una BLOCKCHAIN son posibles, pero por la naturaleza de la tecnología, son muy difíciles de completarse con éxito porque el atacante debería controlar más del 50% de la potencia de hash de la red. Esto permitiría al atacante bloquear la red o revertir transacciones lo que requiere una inversión tecnológica muy alta.

Teniendo en cuenta esta explicación, se expone una tabla comparativa donde se aclararán los conceptos clave de cada tipo de BLOCKCHAIN. Posteriormente, se

realizará una explicación más profunda de cada una de ellas, enfocando los conceptos en sus ventajas y desventajas, así como en su posible aplicación en el comercio electrónico.

En la tabla 1 se puede evidenciar los tipos de BLOCKCHAIN, ventajas y desventajas:

**Tabla 1 Tipos de BLOCKCHAIN**

| Tipo de BLOCKCHAIN | Características Principales |
|---|---|
| BLOCKCHAIN Publico | • Descentralizado<br>• Anónimo<br>• Transacciones transparentes<br>• Alta seguridad<br>• Escalabilidad limitada<br>• Privacidad limitada |
| BLOCKCHAIN Privado | • Descentralizado<br>• Controlado por una organización o entidad específica<br>• Transacciones privadas<br>• Mayor control y confidencialidad<br>• Escalabilidad mejorada. |
| BLOCKCHAIN Federado | • Descentralizado<br>• Controlado por múltiples organizaciones o entidades<br>• Transacciones transparentes<br>• Mayor colaboración y coordinación<br>• Certeza de confianza y seguridad limitadas |
| BLOCKCHAIN Hibrido | • Combina elementos de BLOCKCHAIN público y privado<br>• Descentralizado<br>• Escalable<br>• Regulado<br>• Flexibilidad<br>• Aprovecha las ventajas de ambos tipos de BLOCKCHAIN. |

Fuente: Elaboración Propia

En la figura 4 se puede observar gráficamente los tipos de BLOCKCHAIN[18] y su interconectividad entre nodos que a continuación se explican:

### 6.1.1 BLOCKCHAIN Público

El BLOCKCHAIN público es uno de los tipos más conocidos y utilizados, representado por redes como Bitcoin y Ethereum. En este tipo de BLOCKCHAIN, cualquier persona puede participar y verificar transacciones. Las transacciones son anónimas pero transparentes para todos los participantes de la red. La principal ventaja de un BLOCKCHAIN público es su alta seguridad y descentralización, ya que no hay una autoridad central que controle la red. Sin embargo, su naturaleza abierta puede plantear desafíos en términos de escalabilidad y privacidad, especialmente en el ámbito financiero.

### 6.1.2 BLOCKCHAIN Privado

El BLOCKCHAIN privado, en contraste con el público, se utiliza dentro de una organización o entidad específica. En este caso, la entidad tiene el control y la autoridad sobre la red. Las transacciones son registradas en el BLOCKCHAIN, pero el acceso está restringido a un grupo específico de participantes. Esto proporciona un mayor nivel de privacidad y permite una gestión más ágil de los datos. Un BLOCKCHAIN privado es adecuado para aplicaciones empresariales en las que se requiere un mayor control y confidencialidad en las transacciones financieras.

### 6.1.3 BLOCKCHAIN Federado

El BLOCKCHAIN federado implica la participación de múltiples organizaciones o entidades que tienen autoridad sobre la red. Aunque está descentralizado, es eficiente y escalable en comparación con
el BLOCKCHAIN público. En este tipo de BLOCKCHAIN, las organizaciones involucradas generalmente tienen control sobre la reserva de las transacciones. El BLOCKCHAIN federado se utiliza en casos en los que se requiere una mayor colaboración y coordinación entre múltiples partes interesadas. Sin embargo, también implica cierto grado de centralización, lo que puede plantear desafíos en términos de confianza y seguridad.

### 6.1.4 BLOCKCHAIN Híbrido

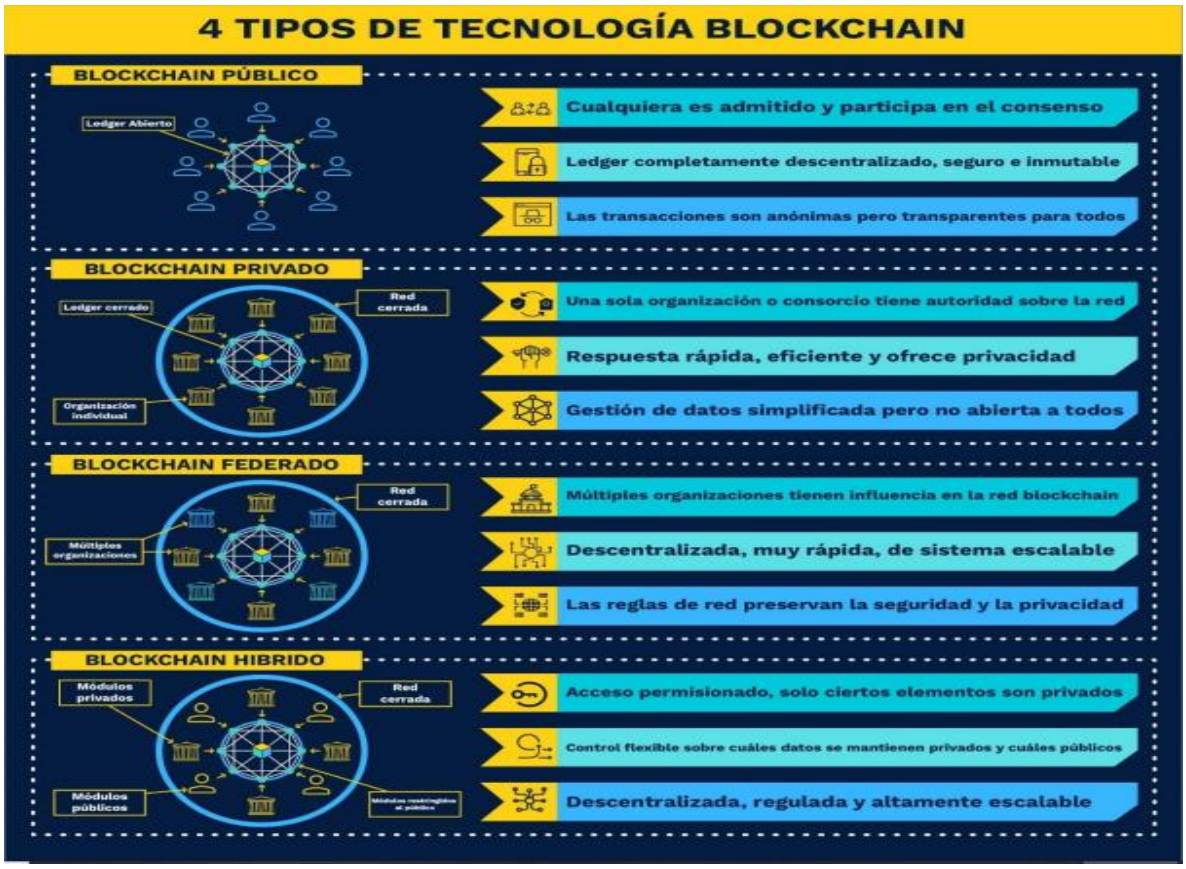
El BLOCKCHAIN híbrido combina elementos de redes públicas y privadas. Puede tener operaciones en modo privado que eventualmente se registran en la red

[18] Fuente: MINTIC Guía de referencia de blockchain para la adopción e implementación de proyectos en el estado colombiano {sitio web} {en línea} {consultado el 21 de octubre de 2023} Disponible en: https://gobiernodigital.mintic.gov.co/692/articles-161810_pdf.pdf

pública. Esta combinación proporciona características descentralizadas, escalabilidad y regulación. Un BLOCKCHAIN híbrido puede ser beneficioso en el contexto de transacciones financieras en el comercio electrónico, ya que brinda flexibilidad y permite aprovechar las ventajas de ambos tipos de BLOCKCHAIN.

Por ejemplo, las transacciones internas pueden gestionarse en un entorno privado, mientras que las transacciones finales se registran en la red pública para mayor transparencia y verificación.

**Figura 4: Grafica tipos de BLOCKCHAIN**




Fuente: https://gobiernodigital.mintic.gov.co/692/articles-161810_pdf.pdf

Como se puede apreciar en la figura y en la tabla descrita anteriormente, cada tipo de BLOCKCHAIN tiene sus propias ventajas y desventajas. El tipo de BLOCKCHAIN más adecuado para una aplicación específica dependerá de una serie de factores, como el nivel de seguridad requerido, la privacidad, la escalabilidad, la flexibilidad y el coste

### 6.1.5 Consideraciones para seleccionar el tipo de BLOCKCHAIN y la normatividad ISO 20022[19]

La norma ISO 20022 es una familia de normas técnicas internacionales que definen un conjunto común de mensajes para el intercambio de información financiera. Esta norma proporciona un marco para el intercambio de mensajes financieros entre las entidades financieras, lo que ayuda a mejorar la eficiencia, la seguridad y la transparencia de las transacciones financieras.

La norma ISO 20022 tiene un alcance amplio, ya que cubre una amplia gama de transacciones financieras, como pagos, remesas, inversiones y seguros. La norma está siendo adoptada gradualmente por las entidades financieras de todo el mundo, y se espera que tenga un impacto significativo en la industria financiera.

Estos son algunos de los beneficios de usar la norma ISO 20022:

**Mayor eficiencia**: la norma ISO 20022 ayuda a mejorar la eficiencia de las transacciones financieras al proporcionar un conjunto común de mensajes que pueden ser utilizados por todas las entidades financieras. Esto reduce la necesidad de volver a codificar los mensajes y facilita el intercambio de información entre las entidades financieras.

**Mayor seguridad**: la norma ISO 20022 ayuda a mejorar la seguridad de las transacciones financieras al proporcionar un conjunto común de mensajes que están diseñados para ser seguros. Esto incluye el uso de firmas digitales y el cifrado para proteger la información financiera.

**Mayor transparencia:** la norma ISO 20022 ayuda a mejorar la transparencia de las transacciones financieras al proporcionar un conjunto común de mensajes que están diseñados para ser claros y fáciles de entender. Esto facilita a los usuarios comprender los términos de las transacciones financieras y tomar decisiones informadas.

La normatividad ISO 20022 tiene un alcance amplio y abarca diversos aspectos que pueden contribuir a reducir los ciberataques a entidades financieras, incluyendo aquellas ubicadas en Colombia. Al adoptar esta norma, las entidades financieras pueden fortalecer su seguridad y protección frente a posibles amenazas cibernéticas. A continuación, se detallan algunos puntos clave sobre el alcance de la normatividad ISO 20022 en relación con la reducción de ciberataques.

[19] Fuente: ULTIMACO, Impacto de norma ISO 20022 en la unión de finanzas tradicionales y cripto, {Sitio web} {en línea} {consultado el 21 de octubre 2023} Disponible en: https://observatorioblockchain.com/criptomonedas/norma-iso-20022-e-impacto-en-union-de-dinero-tradicional-y-cripto/

La última versión de ISO 20022 es la versión 2019, publicada en junio del mismo año. La ISO 20022, es una familia de normas técnicas internacionales para mensajes financieros. Proporcionan un marco para el intercambio de mensajes financieros entre las entidades financieras[20].

La elección del tipo de BLOCKCHAIN para validar transacciones financieras en el comercio electrónico debe basarse en varios factores clave. A continuación, se presentan algunos aspectos para tener en cuenta durante el proceso de selección:

- **Soporte de contratos inteligentes**: Es importante investigar si la BLOCKCHAIN en consideración es compatible con contratos inteligentes. Los contratos inteligentes son programas informáticos autónomos que ejecutan automáticamente las condiciones establecidas en ellos. Su implementación en la BLOCKCHAIN puede ser crucial para el comercio electrónico, ya que permite automatizar y garantizar la ejecución de acuerdos y transacciones.

- **Arquitectura y compatibilidad:** Es fundamental analizar la arquitectura de la BLOCKCHAIN para determinar si es compatible con los requisitos del comercio electrónico. Por ejemplo, la capacidad de escalabilidad, tiempos de confirmación de transacciones y compatibilidad con sistemas existentes son aspectos que deben considerarse.

- **Requisitos de privacidad y seguridad:** La protección de las transacciones financieras es de suma importancia en el comercio electrónico. Por lo tanto, es esencial evaluar si la plataforma de BLOCKCHAIN proporciona un nivel adecuado de seguridad y privacidad para garantizar la confidencialidad de los datos y evitar posibles ataques cibernéticos.

- **Código abierto y colaboración**: Investigar si la plataforma de BLOCKCHAIN es de código abierto puede ser beneficioso, ya que permite una mayor transparencia y colaboración en el desarrollo y la integración con otros sistemas. Esto facilita la revisión y mejora continua de la tecnología, así como la creación de comunidades de desarrollo activas.

- **Interoperabilidad e integración**: La capacidad de integración con otros protocolos, proveedores y desarrolladores es otro aspecto importante por considerar. Una BLOCKCHAIN que permite la interoperabilidad y la

[20] Fuente: GOULD Rick, BANNABY Lewis, LOCKETT Kath, La nueva ola en finanzas {en línea} {enero 2020} {consultado el 25 de julio 2023} disponible en: https://www.iso.org/files/live/sites/isoorg/files/news/magazine/ISOfocus%20(2013-NOW)/sp/ISOfocus_138_sp.pdf

integración con sistemas existentes en el comercio electrónico brinda flexibilidad y facilita la adopción de la tecnología.

- **Estándares de seguridad:** La norma ISO 20022:2019 proporciona directrices y mejores prácticas en materia de seguridad de la información. Establece requisitos para garantizar la confidencialidad, integridad y disponibilidad de los datos financieros. Al implementar estos estándares de seguridad, las entidades financieras pueden fortalecer sus sistemas y reducir las vulnerabilidades que podrían ser explotadas por los ciberdelincuentes.

- **Autenticación y autorización:** La normatividad ISO 20022:2019 incluye mecanismos para la autenticación y autorización de los participantes en las transacciones financieras. Estos mecanismos aseguran que solo las entidades y usuarios autorizados puedan acceder y realizar operaciones en los sistemas financieros. La autenticación robusta y los mecanismos de autorización adecuados son fundamentales para prevenir ataques de suplantación de identidad y accesos no autorizados.

- **Criptografía**: La norma ISO 20022:2019 también aborda aspectos relacionados con la criptografía, que es una herramienta esencial en la protección de datos sensibles en el ámbito financiero. Establece recomendaciones para el uso de algoritmos de cifrado fuertes y prácticas adecuadas en el manejo de claves criptográficas. Al implementar técnicas de criptografía sólidas, las entidades financieras pueden proteger la confidencialidad de los datos y reducir el riesgo de exposición a ciberataque.

- **Gestión de riesgos:** La normatividad ISO 20022:2019 promueve la implementación de un enfoque integral de gestión de riesgos en el ámbito financiero. Proporciona directrices para identificar, evaluar y gestionar los riesgos asociados con las transacciones financieras. Al adoptar un enfoque basado en riesgos, las entidades financieras pueden identificar posibles amenazas cibernéticas y tomar medidas proactivas para mitigar los riesgos.

- **Monitoreo y detección de incidentes:** La norma ISO 20022:2019 también destaca la importancia de contar con sistemas de monitoreo y detección de incidentes en tiempo real. Estos sistemas permiten identificar actividades sospechosas o anómalas en los sistemas financieros y responder de manera oportuna ante posibles ciberataques. Al implementar sistemas de monitoreo y detección robustos, las entidades financieras pueden reducir la exposición a ciberataques y minimizar el impacto de posibles incidentes.

En el contexto de Colombia, la adopción de la normatividad ISO 20022:2019 puede contribuir significativamente a la reducción de ciberataques a entidades financieras.

Al implementar los estándares de seguridad y las mejores prácticas recomendadas por la norma, las entidades financieras colombianas pueden fortalecer su infraestructura tecnológica, proteger la integridad de los datos financieros y mejorar la confianza de los usuarios en los sistemas financieros del país. Además, la adopción de esta norma puede facilitar la colaboración y el intercambio seguro de información financiera entre las entidades financieras colombianas y sus contrapartes internacionales, promoviendo así la seguridad y la estabilidad en el ámbito financiero a nivel global.

Teniendo en cuenta los factores anteriores se puede concluir que la BLOCKCHAIN híbrida sería la opción más recomendada para la validación de transacciones financieras en el comercio electrónico. Su combinación de características descentralizadas y reguladas, junto con la flexibilidad y la posibilidad de aprovechar las ventajas de los BLOCKCHAIN públicos y privados, proporciona eficiencia y seguridad frente a posibles ataques cibernéticos.

La normatividad ISO 20022:2019 ofrece un enfoque integral y estructurado para fortalecer la seguridad y reducir los ciberataques en las entidades financieras. Su implementación puede ayudar a mitigar riesgos, proteger la integridad de los datos financieros y fortalecer la confianza de los usuarios en el sistema financiero.

Al seleccionar el tipo de BLOCKCHAIN para validar transacciones financieras en el comercio electrónico, es fundamental evaluar cuidadosamente las características y requisitos específicos de cada tipo. La elección final debe basarse en una comprensión profunda de las necesidades del negocio, las capacidades de la tecnología BLOCKCHAIN y la normatividad ISO 20022:2019, asegurando así una implementación exitosa y segura en el contexto del comercio electrónico.

Esta combinación de la normatividad ISO 20022:2019 y la selección adecuada del tipo de BLOCKCHAIN brindará eficiencia, confiabilidad y seguridad adecuadas para la validación de transacciones financieras en el comercio electrónico, al tiempo que reducirá los riesgos de ciberataques y fortalecerá la protección de los datos sensibles.

## 6.2 COMPARAR LOS PROTOCOLOS PROOF OF WORK Y PROOF OF STAKE, Y SU MÉTODO DE FUNCIONAMIENTO EN LA VALIDACIÓN DE BLOQUES.

Los algoritmos de consenso[21] son un componente fundamental de las redes BLOCKCHAIN. Estos algoritmos definen cómo se validan las transacciones y se agregan bloques a la cadena. Existen varios algoritmos de consenso, cada uno con sus propias ventajas y desventajas.

**Proof of Work (PoW):** El protocolo PoW es el algoritmo de consenso más utilizado en la actualidad. Es el protocolo utilizado por Bitcoin, Ethereum y otras blockchains populares. En PoW, los nodos de la red compiten para resolver algoritmos criptográficos complejos. El nodo que resuelve el algoritmo primero se le asigna el derecho de validar el bloque siguiente.

Las principales ventajas de PoW son su seguridad y su inmutabilidad. PoW es muy resistente a los ataques, ya que es muy costoso y difícil para un atacante manipular la cadena. Además, PoW garantiza que la cadena es inmutable, ya que es muy difícil revertir un bloque una vez que se ha agregado a la cadena.

Sin embargo, PoW también tiene algunas desventajas. El proceso de resolución de algoritmos es muy intensivo en energía, lo que ha llevado a críticas sobre su sostenibilidad. Además, PoW puede ser muy costoso para los participantes, ya que requieren hardware especializado y recursos informáticos considerables.

**Proof of Stake (PoS):** El protocolo PoS es un algoritmo de consenso alternativo que es más eficiente en energía que PoW. En PoS, los nodos de la red son seleccionados para validar bloques en función de la cantidad de criptomonedas que poseen. Los nodos que poseen más criptomonedas tienen una mayor probabilidad de ser seleccionados para validar bloques.

Las principales ventajas de PoS son su eficiencia energética y su escalabilidad. PoS es mucho más eficiente en energía que PoW, ya que no requiere que los nodos resuelvan algoritmos criptográficos complejos. Además, PoS es más escalable que PoW, ya que no requiere que la red aumente su tamaño para acomodar a más participantes.

Sin embargo, PoS también tiene algunas desventajas. PoS puede ser más centralizado que PoW, ya que los nodos con más criptomonedas tienen más poder en la red. Además, PoS puede ser menos seguro que PoW, ya que es posible que

[21] Fuente: CARDANO, PoS de Cardano vs. PoW de Bitcoin {página web} {en línea} {consultado el 24 de octubre 2023} disponible en: https://forum.cardano.org/t/pos-de-cardano-vs-pow-de-bitcoin/27910

un atacante pueda adquirir una gran cantidad de criptomonedas para manipular la cadena.

**Prueba de Autoridad (Proof of Authority, PoA):** El protocolo PoA[22] es un algoritmo de consenso que se utiliza en blockchains privadas o de consorcios. En PoA, un conjunto de nodos de confianza, conocidos como "autoridades", son los encargados de validar las transacciones y agregar bloques a la cadena. Las autoridades son seleccionadas previamente y tienen un estatus especial en la red.

Sin embargo, PoA también tiene algunas desventajas. PoA puede ser menos descentralizado que otros algoritmos de consenso, ya que las autoridades tienen un mayor poder en la red. Además, PoA puede ser menos escalable que otros algoritmos de consenso, ya que la red está limitada por el número de autoridades.

Como se puede apreciar, los algoritmos de consenso PoW, PoS y PoA tienen sus propias ventajas y desventajas. La elección del algoritmo de consenso más adecuado depende de las necesidades específicas de la aplicación.

Para las aplicaciones que requieren un alto nivel de seguridad e inmutabilidad, el protocolo PoW es una buena opción. Sin embargo, para las aplicaciones que requieren eficiencia energética y escalabilidad, el protocolo PoS o PoA puede ser una mejor opción.

Una plataforma de comercio electrónico podría utilizar PoA para validar las transacciones. Los nodos autorizados podrían ser los proveedores de servicios de pago, los bancos o las instituciones financieras. Esto permitiría a la plataforma de comercio electrónico validar las transacciones de forma rápida y eficiente, sin necesidad de que todos los usuarios participen en el proceso.

Estos son solo algunos ejemplos de algoritmos de consenso utilizados en BLOCKCHAIN. Cada uno tiene sus propias características, ventajas y desventajas en términos de seguridad, escalabilidad y eficiencia.

Al considerar la aplicabilidad de los protocolos de validación de bloques en el comercio electrónico financiero, es esencial evaluar varios aspectos relevantes. Uno de ellos es la eficiencia y escalabilidad de los protocolos, lo cual tiene un impacto directo en la velocidad y el costo de las transacciones. En este sentido, la normativa ISO 9001:2015 puede desempeñar un papel importante al establecer directrices para la gestión de la calidad en los procesos relacionados con el comercio electrónico financiero.

[22] Fuente: ROAMS Finanzas, Proof of authority: que es y como funciona {pagina web} {en línea} {consultado el 24 de octubre 2023} disponible en: https://finanzas.roams.es/academia/criptomonedas/proof-of-authority/

La norma ISO 9001:2015 proporciona un enfoque sistemático para identificar y mejorar los procesos clave involucrados en las transacciones financieras en línea. Esto implica definir y documentar los procedimientos, establecer controles adecuados para garantizar la calidad de las transacciones y medir regularmente el desempeño del sistema. Al cumplir con los requisitos de la norma ISO 9001, las empresas pueden asegurarse de que sus operaciones de comercio electrónico financiero cumplan con altos estándares de calidad y eficiencia.

También, la seguridad y la resistencia a ataques son aspectos críticos en el comercio electrónico financiero. Aquí es donde la normativa ISO 27001 en su versión 2019 cobra importancia. Este estándar establece los requisitos para implementar un sistema de gestión de seguridad de la información, que aborda la identificación y evaluación de riesgos, la implementación de controles adecuados y la mejora continua de la seguridad de la información. Al adoptar la normativa ISO 27001:2019, las organizaciones pueden mitigar los riesgos de seguridad y fortalecer la protección de los datos financieros en sus procesos de validación de bloques.

Además de las normas ISO, también es fundamental tener en cuenta las regulaciones específicas del país o región en la que se realiza el comercio electrónico financiero. Estas regulaciones pueden abordar aspectos como la protección del consumidor, el cumplimiento normativo y la privacidad de los datos financieros. Por ejemplo, en Europa, el Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés) establece requisitos estrictos para el manejo y la protección de datos personales. Las empresas que operan en el comercio electrónico financiero deben asegurarse de cumplir con estas regulaciones para evitar posibles sanciones y garantizar la confianza de los clientes.

El Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés) es una normativa de la Unión Europea que entró en vigor el 25 de mayo de 2018. El objetivo principal del GDPR es fortalecer y unificar la protección de los datos personales de los ciudadanos de la UE, así como garantizar la privacidad y control sobre su información.

El GDPR establece una serie de derechos y principios clave que deben ser respetados por las organizaciones que procesan datos personales. Algunos de los aspectos más destacados del GDPR son:

- **Consentimiento:** El consentimiento del titular de los datos debe ser obtenido de manera clara y explícita antes de recopilar y procesar sus datos personales. Además, el titular tiene el derecho de retirar su consentimiento en cualquier momento.

- **Derechos de los titulares de los datos:** El GDPR otorga a los individuos una serie de derechos, como el derecho de acceso a sus datos

personales, el derecho a rectificar información inexacta, el derecho a ser olvidado (es decir, a solicitar la eliminación de sus datos), el derecho a la portabilidad de los datos y el derecho a oponerse al procesamiento de sus datos en ciertas circunstancias.

- **Responsabilidad y transparencia:** Las organizaciones deben ser transparentes en cuanto a cómo recopilan, utilizan, procesan y almacenan los datos personales. También deben implementar medidas de seguridad adecuadas para proteger los datos contra el acceso no autorizado o la pérdida.

- **Notificación de violaciones de seguridad:** En caso de una violación de seguridad que pueda comprometer los datos personales, las organizaciones están obligadas a notificar a las autoridades de protección de datos y a los individuos afectados en un plazo determinado.

- **Transferencia internacional de datos:** El GDPR establece requisitos específicos para la transferencia de datos personales fuera de la UE, asegurando que se mantengan los mismos niveles de protección de datos.

El incumplimiento del GDPR puede resultar en sanciones financieras significativas para las organizaciones, que pueden ascender a hasta el 4% de su facturación global anual o 20 millones de euros, según la cifra que sea mayor.

Las organizaciones que operan en el comercio electrónico financiero en Europa deben cumplir con los requisitos del GDPR, garantizando la seguridad y privacidad de los datos de los clientes y el cumplimiento normativo adecuado.

En Colombia, el equivalente al GDPR de la Unión Europea es la Ley Estatutaria 1581 de 2012, conocida como la Ley de Protección de Datos Personales. Esta ley tiene como objetivo principal regular el manejo de los datos personales por parte de las entidades públicas y privadas en el territorio colombiano, estableciendo los principios, derechos y obligaciones para garantizar la protección de la privacidad y los derechos de los titulares de los datos.

La Ley de Protección de Datos Personales en Colombia establece una serie de principios fundamentales que deben ser respetados en el tratamiento de datos personales, tales como el principio de finalidad, que implica que los datos deben ser recolectados con un propósito legítimo y específico; el principio de libertad, que garantiza que el titular del dato tenga la opción de suministrar o no su información personal; el principio de veracidad, que exige que los datos sean exactos, completos y actualizados, entre otros.

Además, esta ley reconoce los derechos de los titulares de los datos, como el derecho de acceso, que les permite conocer qué información se está recopilando y cómo se está utilizando; el derecho de rectificación, para corregir datos inexactos o incompletos; el derecho de supresión, para solicitar la eliminación de los datos personales cuando no se cumplan los principios y requisitos establecidos; y el derecho de oposición, que permite al titular oponerse al tratamiento de sus datos en determinadas circunstancias.

La Ley de Protección de Datos Personales también establece la obligación de implementar medidas de seguridad adecuadas para proteger los datos personales contra pérdidas, alteraciones, acceso no autorizado y cualquier forma de tratamiento indebidos.

Las organizaciones que operan en Colombia y manejan datos personales deben cumplir con los requisitos de esta ley y garantizar el cumplimiento normativo adecuado.

La elección entre PoW, PoS y PoA para la validación de bloques en el comercio electrónico debe basarse en una evaluación cuidadosa de los factores mencionados anteriormente. Si la seguridad y la resistencia a ataques son prioritarias, PoW puede ser preferible.

Por otro lado, como se mencionó anteriormente, si la eficiencia, la escalabilidad y la sostenibilidad son más importantes, PoS o PoA pueden ser opciones más adecuadas. La selección del protocolo apropiado también debe considerar los requisitos específicos del contexto de aplicación y los objetivos de la plataforma BLOCKCHAIN.

En la figura 5 se representa la comparación grafica entre los protocolos Pow y PoS.

**Figura 5: Protocolo PoW y PoS**

Fuente: https://forum.cardano.org/t/pos-de-cardano-vs-pow-de-bitcoin/27910

En el comercio electrónico financiero, es importante comprender los diferentes tipos de redes, como la red centralizada, la red descentralizada y la red distribuida, para determinar cuál es la más adecuada en términos de aplicabilidad. A continuación, se exploran cada uno de estos tipos de redes, así como sus ventajas y desventajas:

**Red Centralizada**: En una red centralizada, la autoridad y el control se encuentran en manos de una entidad central. Esta entidad tiene la responsabilidad de gestionar y coordinar todas las actividades de la red. Algunos ejemplos comunes de redes centralizadas son los sistemas bancarios tradicionales y las plataformas de pago centralizadas.

**Ventajas:**

**Eficacia y toma de decisiones rápidas**: En una red centralizada, la toma de decisiones puede ser rápida y eficiente, ya que la entidad central tiene el control total sobre la red y puede implementar cambios y mejoras de manera más ágil.
Mantenimiento y soporte simplificados: Al ser responsables de toda la red, las entidades centrales pueden proporcionar un mantenimiento y soporte más centralizados, lo que facilita la resolución de problemas y la implementación de actualizaciones.

**Desventajas:**

**Puntos únicos de falla y vulnerabilidad:** Si la entidad central experimenta una falla o es atacada, toda la red puede quedar comprometida. Esto puede resultar en la interrupción de los servicios y la pérdida de confianza de los usuarios.
Falta de transparencia y confianza: En una red centralizada, los usuarios deben confiar en la entidad central para gestionar adecuadamente los datos y garantizar la seguridad. Esto puede plantear preocupaciones sobre la privacidad y la falta de transparencia en las operaciones.

**Red Descentralizada:** En una red descentralizada, no hay una entidad central que controle o coordine todas las actividades. En cambio, las decisiones y el control se distribuyen entre múltiples nodos o participantes de la red. Ejemplos de redes descentralizadas incluyen algunas plataformas de criptomonedas y sistemas peer-to-peer.

**Ventajas:**

**Mayor resistencia y redundancia:** La descentralización reduce la dependencia de un solo punto de falla. Si un nodo o participante falla, otros pueden seguir operando, lo que aumenta la resistencia y la disponibilidad de la red.

**Mayor transparencia y confianza**: Al eliminar la necesidad de confiar en una entidad central, una red descentralizada puede proporcionar mayor transparencia y confianza, ya que las transacciones y los registros pueden ser verificados y validados por múltiples participantes de la red.

**Desventajas:**

**Toma de decisiones más lenta:** En una red descentralizada, se requiere llegar a un consenso entre los diferentes nodos o participantes para tomar decisiones importantes. Esto puede llevar más tiempo y dificultar la implementación de cambios rápidos.

**Requerimientos técnicos y participación:** La participación en una red descentralizada puede requerir conocimientos técnicos y recursos adicionales, lo que puede limitar la accesibilidad y la adopción masiva.

**Red Distribuida:** En una red distribuida, la información y las tareas se distribuyen entre múltiples nodos de manera igualitaria. Cada nodo tiene una copia completa de la red y puede realizar tareas de procesamiento y validación de manera independiente. La tecnología BLOCKCHAIN es un ejemplo prominente de una red distribuida.

**Ventajas:**

**Alta seguridad y resistencia a ataques**: En una red distribuida, la información se almacena en múltiples nodos, lo que dificulta la manipulación y el ataque de la red. Esto la hace especialmente adecuada para aplicaciones financieras que requieren un alto nivel de seguridad.

**Transparencia y trazabilidad:** Las redes distribuidas, como BLOCKCHAIN, ofrecen transparencia y trazabilidad al registrar todas las transacciones en un libro de contabilidad inmutable y compartido. Esto brinda confianza a los participantes y permite una mayor visibilidad de las operaciones.

**Desventajas:**

**Consumo de recursos**: Las redes distribuidas, especialmente las basadas en BLOCKCHAIN, pueden requerir una gran cantidad de recursos computacionales y energéticos para mantener la integridad de la red. Esto puede resultar en costos operativos más altos.

**Escalabilidad:** La escalabilidad en una BLOCKCHAIN se refiere a la capacidad de la red para manejar un crecimiento en el número de transacciones y usuarios de manera eficiente, sin comprometer la velocidad de confirmación de las transacciones ni aumentar significativamente los costos.

En el contexto de las BLOCKCHAIN, la escalabilidad es un desafío importante debido a la naturaleza distribuida y descentralizada de la tecnología. Las BLOCKCHAIN más conocidas, como Bitcoin y Ethereum, han experimentado problemas de escalabilidad a medida que aumentaba su adopción.

Existen diferentes enfoques para abordar la escalabilidad en las BLOCKCHAIN:

1. **Aumento del tamaño del bloque:** En BLOCKCHAIN como Bitcoin, el tamaño del bloque determina cuántas transacciones pueden incluirse en un bloque. Aumentar el tamaño del bloque puede permitir una mayor capacidad de transacciones, pero también puede aumentar la carga de almacenamiento y ancho de banda requeridos para mantener la red.

A medida que una red distribuida crece en tamaño y volumen de transacciones, puede enfrentar desafíos de escalabilidad debido a la necesidad de sincronización y consenso entre los nodos.

2. **Mejoras en el algoritmo de consenso:** El algoritmo de consenso utilizado por una BLOCKCHAIN puede afectar su capacidad de escalabilidad. Por ejemplo, Bitcoin utiliza el algoritmo de consenso de Prueba de Trabajo (PoW), que puede limitar la velocidad de confirmación de las transacciones.

Otros algoritmos de consenso, como la Prueba de Participación (PoS) o la Prueba de Autoridad (PoA), pueden ofrecer una mayor eficiencia en términos de escalabilidad.

3. **Soluciones de capa 2:** Una solución de capa 2 es una técnica o enfoque utilizado en BLOCKCHAIN para aumentar la capacidad y la escalabilidad de la red al realizar transacciones fuera de la cadena principal. Estas soluciones se implementan como capas adicionales en la parte superior de la cadena de bloques existente y se utilizan para procesar un gran número de transacciones de forma más eficiente y rápida.

   El objetivo principal de las soluciones de capa 2 es aliviar la carga en la cadena principal y reducir las limitaciones de escalabilidad inherentes a las BLOCKCHAIN. Al mover una gran cantidad de transacciones fuera de la cadena principal, estas soluciones permiten un procesamiento más rápido y menos costoso.
   Algunas de las soluciones de capa 2 más conocidas son:

   - **Lightning Network**: Es una solución de capa 2 para Bitcoin. Permite realizar transacciones rápidas y de bajo costo al establecer canales de pago fuera de la cadena principal de Bitcoin. Estos canales permiten a los participantes realizar transacciones privadas y sin confirmaciones inmediatas, lo que reduce la carga en la cadena principal y mejora la escalabilidad de Bitcoin.

   - **Raiden Network:** Similar a Lightning Network, Raiden Network es una solución de capa 2 para Ethereum. Permite realizar transacciones rápidas y de bajo costo a través de canales de estado fuera de la cadena. Con Raiden Network, los usuarios pueden realizar pagos instantáneos y escalables sin tener que esperar confirmaciones en la cadena principal de Ethereum.

   - **Plasma:** Es una solución de capa 2 que permite la creación de cadenas laterales (sidechains) que están conectadas a la cadena principal. Estas cadenas laterales pueden procesar un gran número de transacciones de manera independiente y luego informar a la cadena principal de los resultados. Plasma mejora la escalabilidad al reducir la carga en la cadena principal de la BLOCKCHAIN.

   - **State Channels:** Son canales de comunicación fuera de la cadena que permiten a los participantes realizar múltiples transacciones sin tener que registrar cada una de ellas en la cadena principal. Estos canales mantienen un estado compartido entre los participantes y solo registran

las transacciones finales en la cadena principal, lo que mejora la eficiencia y la escalabilidad.

Estas soluciones de capa 2 ofrecen ventajas significativas en términos de velocidad, capacidad y costo en comparación con las transacciones realizadas directamente en la cadena principal. Sin embargo, también presentan desafíos técnicos y requieren un diseño y una implementación cuidadosa para garantizar la seguridad y la confianza en el sistema.

4. **Blockchain de fragmentación:** Esta solución implica dividir la BLOCKCHAIN en fragmentos más pequeños o cadenas laterales (sidechains), cada uno de los cuales puede procesar transacciones de manera independiente. Esto permite una mayor capacidad de transacciones y una mayor escalabilidad global.

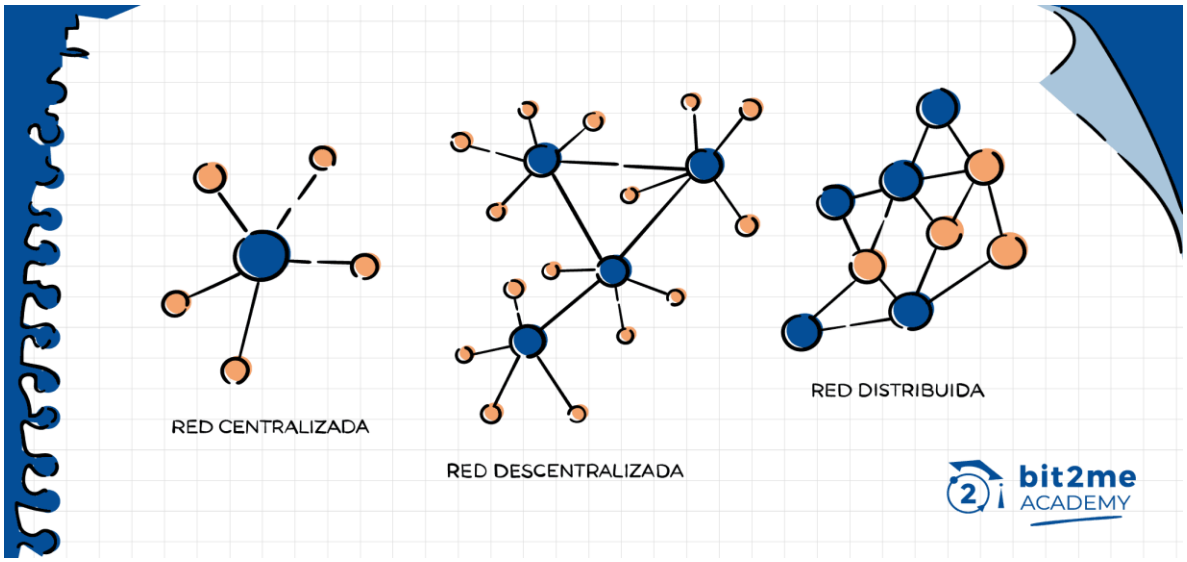
Es importante destacar que la escalabilidad en las BLOCKCHAIN sigue siendo un área de investigación y desarrollo activa, y se están explorando constantemente nuevas soluciones y mejoras para abordar este desafío.

En cuanto a la aplicabilidad en el comercio electrónico financiero, la red distribuida, como BLOCKCHAIN, se considera una opción altamente relevante.

Proporciona una mayor seguridad, transparencia y trazabilidad en las transacciones financieras, lo que es fundamental para establecer la confianza en un entorno comercial en línea. Además, la capacidad de mantener registros inmutables y compartir datos de manera segura puede ser beneficioso para el cumplimiento normativo y la resolución de disputas. Sin embargo, es importante considerar los requisitos específicos de la plataforma y evaluar las ventajas y desventajas de cada tipo de red antes de tomar una decisión final.

En la figura 6 se representan gráficamente los tipos de redes mencionados.

**Figura 6: Tipos de redes**




Fuente: https://academy.bit2me.com/tipos-redes-criptomonedas/

## ALGUNOS MEDIOS DE PAGO DIGITAL UTILIZADOS EN COLOMBIA

**PSE**:

En Colombia, la red PSE (Pago Seguro en Línea) es un sistema de pagos electrónicos utilizado ampliamente para realizar transacciones financieras en línea de manera segura y conveniente. PSE es una iniciativa liderada por la Asociación Bancaria y de Entidades Financieras de Colombia (ASOBANCARIA) en colaboración con los bancos y entidades financieras del país.

El funcionamiento de la red PSE se basa en la conexión entre los comercios electrónicos, los bancos y los usuarios finales. A continuación, se describen los pasos involucrados en una transacción típica a través de la red PSE:

**Selección de PSE como método de pago**: En el proceso de compra en un comercio electrónico en Colombia, el usuario selecciona la opción de pago a través de PSE como método preferido.

**Selección del banco:** Una vez seleccionado PSE, el usuario elige su banco o entidad financiera con la cual tiene una cuenta activa.
Redireccionamiento al portal del banco: Después de seleccionar el banco, el usuario es redireccionado al portal en línea de la entidad financiera para continuar con la transacción.

**Autenticación y verificación:** En el portal del banco, el usuario debe autenticarse utilizando sus credenciales de acceso, como su número de cuenta y contraseña, o mediante otros métodos de seguridad adicionales, como tokens o claves de un solo uso denominado también clave dinámica.

**Autorización de la transacción:** Una vez autenticado, el usuario revisa los detalles de la transacción, como el monto a pagar y el beneficiario, y proporciona su consentimiento para autorizar la transacción.

**Confirmación de pago:** Después de la autorización, el banco verifica la disponibilidad de fondos en la cuenta del usuario y realiza la transferencia de fondos al comercio electrónico correspondiente.
Confirmación de la transacción: Una vez que se ha realizado la transferencia de fondos, tanto el usuario como el comercio electrónico reciben una confirmación de la transacción exitosa. El comercio electrónico puede proceder entonces a completar el proceso de compra y enviar los productos o servicios solicitados al usuario.

La red PSE ofrece varias ventajas tanto para los usuarios como para los comercios electrónicos en Colombia. Algunas de estas ventajas son:

**Seguridad:** La red PSE utiliza protocolos de seguridad avanzados para proteger la información financiera y personal de los usuarios durante las transacciones en línea.

**Conveniencia:** Permite a los usuarios realizar pagos electrónicos directamente desde sus cuentas bancarias, evitando la necesidad de utilizar tarjetas de crédito o débito.

**Amplia cobertura:** La red PSE está respaldada por numerosos bancos y entidades financieras en Colombia, lo que garantiza una amplia cobertura y disponibilidad para los usuarios.

**Reducción de costos:** Para los comercios electrónicos, el uso de la red PSE puede ser más económico en comparación con otros métodos de pago, como las tarjetas de crédito, debido a las tarifas más bajas asociadas.

La red PSE en Colombia, es un sistema de pagos electrónicos que permite a los usuarios realizar transacciones en línea de manera segura y conveniente utilizando sus cuentas bancarias. Proporciona una alternativa confiable y ampliamente aceptada para los métodos de pago tradicionales, y contribuye al crecimiento del comercio electrónico en el país.

El sistema PSE utiliza una infraestructura centralizada que facilita las transacciones en línea y la transferencia de fondos entre las cuentas bancarias de los usuarios y los comercios electrónicos. Los pagos a través de PSE se realizan mediante una

conexión segura entre el portal del banco o entidad financiera y el comercio electrónico correspondiente.

Si se desea implementar una BLOCKCHAIN para reforzar la seguridad en un sistema de pagos como PSE, se deben considerar varios factores para determinar la opción más conveniente. Algunas de las BLOCKCHAIN populares que se podrían considerar son:

**Ethereum**: Como se mencionó anteriormente, Ethereum es una plataforma BLOCKCHAIN ampliamente utilizada que admite la ejecución de contratos inteligentes. Ofrece flexibilidad y permite la creación de aplicaciones descentralizadas (DApps) que podrían integrarse con el sistema PSE. Además, Ethereum tiene una comunidad activa y una infraestructura sólida.

**Hyperledger Fabric**[23]: Hyperledger Fabric es una plataforma BLOCKCHAIN empresarial desarrollada por la Fundación Linux. Está diseñada para aplicaciones empresariales y ofrece características como la privacidad, el control de acceso y la capacidad de implementar soluciones personalizadas. Hyperledger Fabric podría ser una opción adecuada si se busca una BLOCKCHAIN privada y controlada por un consorcio de entidades financieras.

**Ripple**[24]: Ripple es una plataforma BLOCKCHAIN centrada en soluciones de pagos y remesas transfronterizas. Ofrece una red de pagos en tiempo real y una criptomoneda llamada XRP. Si se busca una solución de pagos eficiente y rápida para el sistema PSE, Ripple podría ser una opción para considerar.

**Stellar**[25]: Stellar es otra plataforma BLOCKCHAIN que se centra en los pagos y las transferencias de activos. Es conocida por su capacidad de liquidación rápida y su bajo costo de transacción. Stellar podría ser una opción adecuada si se desea una solución eficiente y económica para los pagos en el sistema PSE.

**NEQUI:**

Nequi es una plataforma financiera digital desarrollada por BANCOLOMBIA, uno de los principales bancos de Colombia. La plataforma Nequi permite a los usuarios realizar diversas operaciones financieras a través de su teléfono móvil, sin necesidad de acudir a una sucursal bancaria física.

---

[23] HYPERLEDGER FOUNDATION A Blockchain Platform for the Enterprise {Sitio web}{Consultado el 25 de mayo 2023} Disponible en: https://hyperledger-fabric.readthedocs.io/en/release-2.5/

[24] XRP LEDGER {Sitio web} {Consultado el 25 de mayo 2023} Disponible en: https://xrpl.org/

[25] STELLAR Stellar is an open network for storing and moving money {Sitio web} {Consultado el 25 de mayo 2023} Disponible en: https://www.stellar.org/

A continuación, se explica cómo funciona Nequi en términos generales:
Registro y descarga de la aplicación: Los usuarios interesados en utilizarla deben descargar la aplicación móvil desde la tienda de aplicaciones de su dispositivo (iOS o Android). Luego, se procede al registro en la plataforma proporcionando la información requerida, como nombre, número de teléfono y correo electrónico.

**Creación de una cuenta:** Una vez registrado, el usuario crea una cuenta vinculando su número de teléfono móvil. Además, se puede asociar una tarjeta de débito o crédito para realizar transacciones cuando se valida el registro.

**Funciones básicas**: Nequi ofrece una variedad de funciones financieras básicas que los usuarios pueden utilizar a través de la aplicación. Estas incluyen:
Depósitos y retiros de dinero: Los usuarios pueden realizar depósitos desde una cuenta bancaria tradicional o a través de servicios de recarga. Asimismo, es posible retirar dinero en efectivo a través de cajeros automáticos o puntos de retiro autorizados.

**Envío y recepción de dinero:** Permite a los usuarios enviar dinero a otros usuarios de Nequi o a cuentas bancarias tradicionales en Colombia. También se pueden recibir transferencias de dinero de otros usuarios o entidades.
Pagos de servicios: Los usuarios pueden realizar pagos de servicios básicos, como servicios públicos, telefonía, televisión por cable, entre otros, directamente desde la aplicación.

**Compras en línea**: Ofrece la posibilidad de realizar compras en línea utilizando los fondos disponibles en la cuenta del usuario.

**Ahorro:** La plataforma permite a los usuarios crear metas de ahorro y establecer fondos para alcanzar esos objetivos a través de aportes periódicos.

**Seguridad:** Implementa medidas de seguridad para proteger la información y las transacciones de los usuarios. Estas incluyen el uso de contraseñas seguras, autenticación de dos factores y notificaciones de actividad en la cuenta.

**Atención al cliente:** Proporciona atención al cliente a través de diferentes canales, como chat en línea y soporte telefónico, para resolver consultas y brindar asistencia a los usuarios.

Nequi, como plataforma financiera digital, no utiliza explícitamente la tecnología BLOCKCHAIN como respaldo para sus operaciones. Es una aplicación móvil desarrollada por Bancolombia que utiliza infraestructuras y sistemas bancarios tradicionales para respaldar sus transacciones financieras.

Sin embargo, es importante tener en cuenta que el banco matriz, BANCOLOMBIA, ha estado explorando[26] y adoptando tecnologías emergentes, incluyendo BLOCKCHAIN, en varios aspectos de sus operaciones. Aunque no hay información pública que indique que Nequi esté respaldada directamente por una BLOCKCHAIN, es posible que Bancolombia utilice esta tecnología en otros proyectos o iniciativas relacionadas con la innovación financiera.

**DAVIPLATA:**

DaviPlata es una plataforma financiera digital en Colombia que permite a los usuarios realizar operaciones financieras a través de su teléfono móvil de forma fácil y segura. La plataforma es desarrollada y respaldada por el Grupo Bancolombia, uno de los principales grupos financieros del país.
A continuación, se explica el funcionamiento básico:

**Registro y descarga de la aplicación:** Los usuarios interesados en utilizar DaviPlata deben descargar la aplicación móvil desde la tienda de aplicaciones de su dispositivo (disponible para iOS y Android). Luego, se procede al registro en la plataforma proporcionando la información requerida, como nombre, número de teléfono y correo electrónico.

**Creación de una cuenta:** Una vez registrado, el usuario crea una cuenta en vinculando su número de teléfono móvil. Además, se puede asociar una tarjeta de débito o crédito para realizar transacciones desde la cuenta.

**Funciones básicas:** Ofrece una variedad de funciones financieras que los usuarios pueden realizar a través de la aplicación. Estas incluyen:
Depósitos y retiros de dinero: Los usuarios pueden realizar depósitos en su plataforma, desde una cuenta bancaria tradicional o a través de servicios de recarga disponibles en Colombia. Asimismo, es posible realizar retiros de dinero en efectivo en cajeros automáticos o establecimientos autorizados.

**Envío y recepción de dinero**: Permite a los usuarios enviar dinero a otros usuarios a cuentas bancarias tradicionales en Colombia.
También es posible recibir transferencias de dinero de otros usuarios o entidades.

**Pagos de servicios**: Los usuarios pueden realizar pagos de servicios básicos, como servicios públicos, telefonía, televisión por cable, entre otros, directamente desde la aplicación.

[26] Fuente: BANCOLOMBIA, Blockchain que es y sus diferentes usos más allá de las criptomonedas {noviembre 8 de 2019} {en línea} {Consultado el 27 de junio 2023} Disponible en: https://www.bancolombia.com/wps/portal/innovacion/economia-digital/blockchain

**Compras en línea**: Ofrece la posibilidad de realizar compras en línea utilizando los fondos disponibles en la cuenta del usuario.

**Ahorro:** La plataforma permite a los usuarios crear metas de ahorro y establecer fondos para alcanzar esos objetivos a través de aportes periódicos.

**Seguridad:** Implementa medidas de seguridad para proteger la información y las transacciones de los usuarios. Esto incluye el uso de contraseñas seguras, autenticación de dos factores y notificaciones de actividad en la cuenta.

**Atención al cliente:** Proporciona soporte al cliente a través de diferentes canales, como chat en línea, correo electrónico y líneas telefónicas, para resolver consultas y brindar asistencia a los usuarios.

Para mejorar la seguridad de las transacciones en plataformas como DaviPlata, se podría considerar el uso de una BLOCKCHAIN privada o de consorcio. Estos tipos de BLOCKCHAIN ofrecen mayor control y seguridad sobre las transacciones y la información almacenada.

Una BLOCKCHAIN privada permite limitar el acceso a un grupo específico de participantes que son confiables y autorizados. En este caso, DaviPlata podría implementar una BLOCKCHAIN privada donde solo los participantes autorizados, como el Grupo Bancolombia y los proveedores de servicios asociados, tengan acceso para realizar y verificar las transacciones.

Por otro lado, una BLOCKCHAIN de consorcio es una variante de BLOCKCHAIN privada en la cual múltiples organizaciones participan en el consenso y la validación de transacciones. Este enfoque podría ser beneficioso si la plataforma busca involucrar a otros actores relevantes en el ecosistema financiero colombiano, como otras instituciones bancarias o proveedores de servicios financieros.

Ambos tipos de BLOCKCHAIN privada y de consorcio ofrecen ventajas en términos de seguridad, ya que la información se almacena de manera inmutable y transparente, y las transacciones son validadas por múltiples participantes de confianza. Además, se pueden implementar medidas adicionales de seguridad, como encriptación de datos, para fortalecer la protección de la información confidencial.

Una de las BLOCKCHAIN de consorcio más conocidas y ampliamente utilizadas es Hyperledger Fabric. Hyperledger Fabric, mencionada anteriormente, es un proyecto de código abierto desarrollado por la Fundación Linux que proporciona una plataforma flexible y escalable para la creación de redes BLOCKCHAIN empresariales.

Hyperledger Fabric es especialmente adecuada para aplicaciones empresariales que requieren un mayor grado de privacidad y control. Algunas de las características clave de Hyperledger Fabric incluyen:

**Modelos de participación flexibles**: Permite la creación de una red de consorcio donde múltiples organizaciones pueden participar y colaborar en la validación y ejecución de transacciones. Cada organización puede tener diferentes roles y niveles de autoridad dentro de la red.

**Canalización de transacciones:** Permite la creación de canales privados en la red, donde las transacciones específicas solo son visibles para las partes involucradas en ese canal en particular. Esto brinda mayor privacidad y confidencialidad a las transacciones comerciales.

**Consenso modular**: Hyperledger Fabric admite varios algoritmos de consenso, lo que permite a los miembros del consorcio seleccionar el algoritmo que mejor se adapte a sus necesidades, ya sea utilizando consenso de tolerancia a fallas bizantinas[27] (PBFT), consenso de prueba de autoridad[28] (PoA) u otros.
Modelos de confidencialidad y políticas de acceso: Permite establecer políticas de acceso y confidencialidad para los datos y transacciones dentro de la red, lo que garantiza que solo las partes autorizadas puedan acceder a la información relevante.

Soporte para contratos inteligentes: Hyperledger Fabric utiliza el concepto de "chaincode", que son programas que se ejecutan en la red BLOCKCHAIN para definir y gestionar la lógica empresarial y los contratos inteligentes.

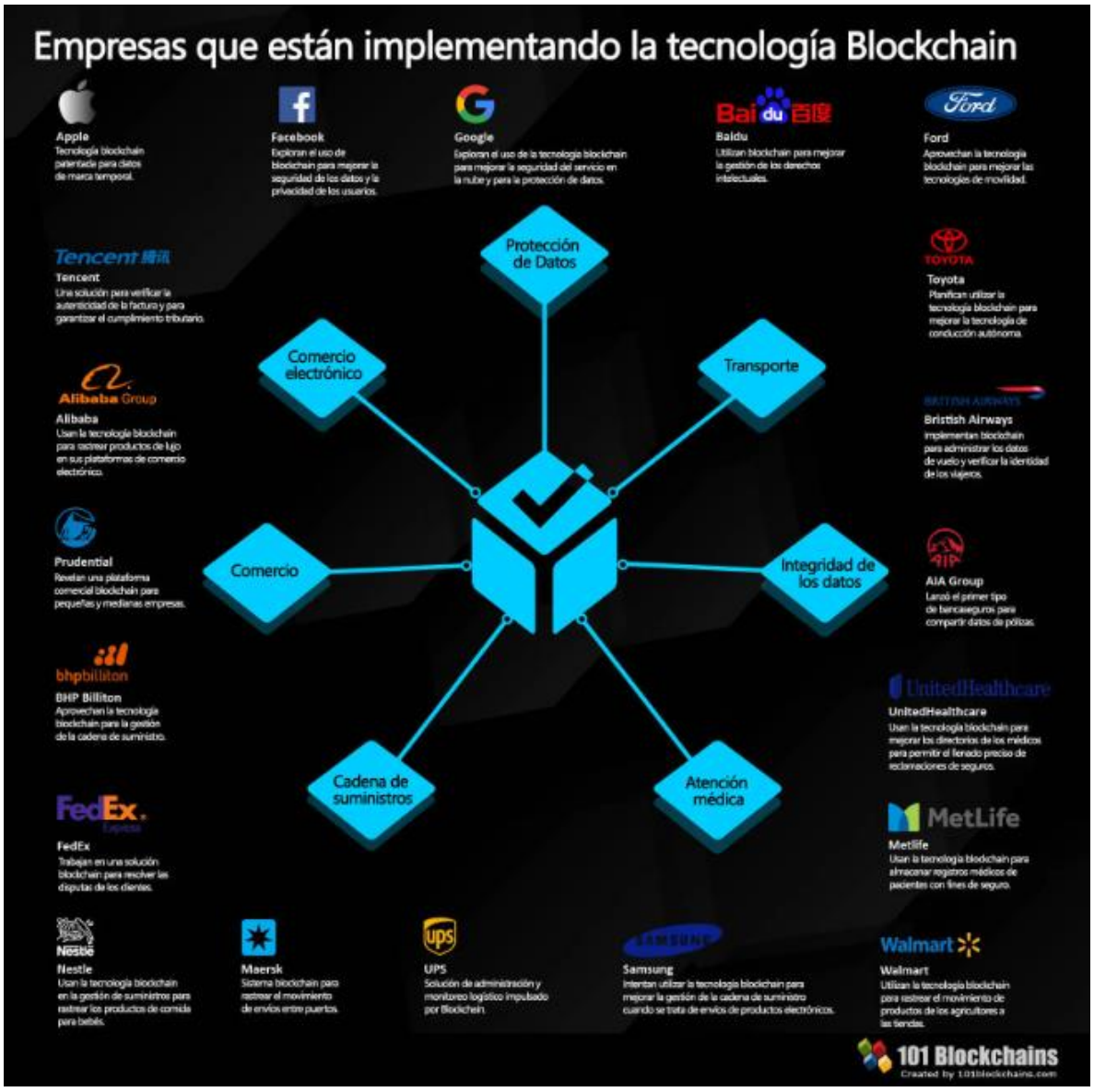
Estas características hacen de Hyperledger Fabric una opción atractiva para aplicaciones empresariales que requieren un mayor nivel de control y privacidad en una red de consorcio. Además, al ser un proyecto de código abierto, ofrece una comunidad activa y un ecosistema de desarrollo sólido.

Es importante destacar que, antes de seleccionar una BLOCKCHAIN de consorcio, es recomendable realizar un análisis detallado de los requisitos específicos del caso de uso, evaluar las características y capacidades de varias opciones disponibles, y considerar factores como la escalabilidad, la seguridad y la interoperabilidad con otros sistemas.

[27] CIBERSEGURIDAD, {Sitio web} Tolerancia a las fallas bizantinas, una guía rápida {Consultado el 26 de mayo 2023} Disponible en: https://ciberseguridad.com/guias/nuevas-tecnologias/criptomoneda/tolerancia-fallas-bizantinas/
[28] BINANCE ACADEMY, {Sitio web} Proof Of Authority {Consultado el 26 de mayo 2023} Disponible en: https://academy.binance.com/es/articles/proof-of-authority-explained

En la figura 7 se representan algunas empresas multinacionales que utilizan tecnología BLOCKCHAIN:

**Figura 7: 20 Empresas que utilizan BLOCKCHAIN**




Fuente: https://101blockchains.com/es/empresas-implementando-blockchain/

La tecnología BLOCKCHAIN todavía está en sus primeras etapas de desarrollo, pero tiene el potencial de revolucionar la industria financiera. La implementación de la tecnología BLOCKCHAIN en las transacciones bancarias podría mejorar significativamente la ciberseguridad y reducir los costos.

De hecho, un estudio realizado por la Universidad de Cambridge encontró que la tecnología BLOCKCHAIN podría reducir el costo de la prevención de fraudes hasta en un 70%[29]. El estudio también encontró que la tecnología BLOCKCHAIN podría reducir el tiempo de procesamiento de las transacciones hasta en un 90%.

La implementación de BLOCKCHAIN en transacciones financieras en Colombia podría mejorar significativamente en términos de eficiencia, seguridad y transparencia.

En cuanto a la eficiencia, BLOCKCHAIN podría reducir los costos de transacción y el tiempo de procesamiento. Esto se debe a que BLOCKCHAIN es una tecnología descentralizada que no requiere intermediarios. Esto significa que las transacciones pueden ser procesadas más rápido y con menos costos.

En cuanto a la seguridad, BLOCKCHAIN es una tecnología muy segura. Esto se debe a que las transacciones en BLOCKCHAIN están encriptadas y verificadas por una red de nodos. Esto hace que sea muy difícil hackear o manipular las transacciones como se explicó anteriormente.

Finalmente, BLOCKCHAIN podría mejorar la transparencia de las transacciones financieras. Esto se debe a que las transacciones en BLOCKCHAIN son públicas y registradas en un libro mayor descentralizado. Esto significa que cualquiera puede ver las transacciones, lo que puede ayudar a prevenir el fraude y el lavado de dinero.

Aquí hay algunos ejemplos específicos de cómo BLOCKCHAIN podría mejorar las transacciones financieras en Colombia:

Los bancos podrían usar BLOCKCHAIN para procesar pagos más rápido y con menos costos. Esto podría beneficiar a los consumidores, ya que podrían pagar sus facturas y hacer transferencias de dinero más rápido y con menos tarifas.

Las empresas podrían usar BLOCKCHAIN para rastrear sus inventarios y productos. Esto podría ayudar a reducir el desperdicio y el fraude.

el gobierno podría usar BLOCKCHAIN para almacenar y compartir datos de manera segura. Esto podría ayudar a mejorar la eficiencia y la transparencia.

Teniendo en cuenta lo anterior, los problemas que se han generado últimamente en el fraude transaccional y el tipo de plataformas que maneja el sistema financiero de Colombia, la implementación de BLOCKCHAIN, podría tener un impacto positivo en

[29] Fuente: HILEMAN Garrick, RAUCHS Michel {Sitio web} {en línea} GLOBAL BLOCKCHAIN BENCHMARKING STUDY UNIVERSITY OF CAMBRIDGE {Consultado el 25 de julio 2023} disponible en: https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2017-09-27-ccaf-globalbchain.pdf

la economía. Podría reducir los costos, mejorar la seguridad y aumentar la transparencia.

Para el comercio electrónico en Colombia, el tipo de blockchain más recomendable para mejorar la seguridad financiera es **Proof of Authority (PoA).** PoA es un algoritmo de consenso que se basa en la confianza de un conjunto de autoridades predeterminadas. Estas autoridades son responsables de validar las transacciones y agregar bloques a la cadena.

PoA es una buena opción para el comercio electrónico en Colombia por las siguientes razones:

**Seguridad:** PoA es muy seguro, ya que las autoridades son seleccionadas por su reputación y confiabilidad. Esto hace que sea muy difícil para un atacante manipular la cadena.

**Eficiencia:** PoA es muy eficiente, ya que no requiere que los nodos resuelvan algoritmos criptográficos complejos. Esto reduce los costos operativos y el consumo de energía.

**Descentralización:** PoA puede ser tan descentralizado como se desee, dependiendo del número de autoridades que se seleccionen.

Otros algoritmos de consenso, como Proof of Work (PoW) y Proof of Stake (PoS), también pueden ser adecuados para el comercio electrónico en Colombia. Sin embargo, PoA ofrece una combinación de seguridad, eficiencia y descentralización que lo hace especialmente atractivo para esta aplicación.

A continuación, se presentan algunos detalles adicionales sobre las ventajas de PoA para el comercio electrónico en Colombia:

**Seguridad:** PoA es muy seguro, ya que las autoridades son seleccionadas por su reputación y confiabilidad. Esto hace que sea muy difícil para un atacante manipular la cadena. En el contexto del comercio electrónico, la seguridad es un factor clave para los consumidores y los comerciantes. PoA puede ayudar a garantizar que las transacciones sean seguras y confiables.

**Eficiencia:** PoA es muy eficiente, ya que no requiere que los nodos resuelvan algoritmos criptográficos complejos. Esto reduce los costos operativos y el consumo de energía. En el contexto del comercio electrónico, la eficiencia es importante para los comerciantes. PoA puede ayudar a reducir los costos y mejorar la rentabilidad.

**Descentralización**: PoA puede ser tan descentralizado como se desee, dependiendo del número de autoridades que se seleccionen. Esto puede ayudar a garantizar que la red sea resistente a la censura y al control centralizado. En el

contexto del comercio electrónico, la descentralización puede ayudar a proteger a los consumidores y los comerciantes de la manipulación de los datos.

## 6.3 EXPLICAR MEDIANTE CASOS EXITOSOS, COMO EL E-COMMERCE RESPALDADO POR UNA BLOCKCHAIN OFRECE UNA ALTA CONFIABILIDAD DE TRANSACCIONES FINANCIERAS DE DIFERENTES ACTIVOS.

A pesar de las limitaciones técnicas y del poco conocimiento de la tecnología en Colombia, se pueden encontrar algunos casos exitosos de implementación de BLOCKCHAIN, algunos de estos son:

- **Caso 1[30]:** La Clínica Las Américas Auna de Medellín anunció una solución sin precedentes para el sector salud y para el cuidado de los pacientes en Colombia. Se trata del uso de la tecnología **IBM Blockchain**, para el seguimiento, control y abastecimiento de dispositivos médicos como catéteres, marcapasos, entre otros. Con la implementación de esta solución de tecnología BLOCKCHAIN, se consiguió reducir a tan solo **24 horas las entregas de insumos**, en un 90% el tiempo de facturación y en un 60% los errores en las órdenes de compra, impactando positivamente el suministro de insumos como catéteres y marcapasos para urgencias vitales.

**Figura 8: Clínica Medellín**

Fuente: https://www.portafolio.co/economia/colombia-estrena-blockchain-para-aparatos-medicos-541689

[30] Fuente: PORTAFOLIO, Colombia estrena blockchain para aparatos médicos {página web} {en línea} {consultado el 21 de octubre 2023}, disponible en: https://www.portafolio.co/economia/colombia-estrena-blockchain-para-aparatos-medicos-541689

- **Caso 2**[31]: Terminal de contenedores de Buenaventura: se convirtió en el primer puerto del país en usar BLOCKCHAIN para realizar seguimiento detallado a la mercancía que se transporta utilizando la plataforma TradeLens[32] que procesa 10 millones de eventos a la semana a nivel mundial, se va generando una cadena de suministro que se alimenta con los datos de carga y descarga de los contenedores[33].

**Figura 9 Terminal marítimo Buenaventura**

Fuente: Diario la Republica

[31] Fuente: LR, IBM se unió con Tcbuen para hacer seguimiento a la carga que pasa por la terminal {página web} {en línea} {consultado el 21 de octubre 2023} disponible en: https://www.larepublica.co/empresas/ibm-se-unio-con-tcbuen-para-hacer-seguimiento-a-la-carga-que-pasa-por-la-terminal-2868824

[32] Fuente: TRADELENS Supply chains are challenged. Its time for new ideas {página web} {en línea} {consultado el 28 de junio 2023} disponible en: https://www.tradelens.com/

[33] Fuente: LA REPUBLICA Tres usos del blockchain más allá del bitcoin {1 junio 2019} {en línea} {consultado el 28 de junio 2023} disponible en: https://www.larepublica.co/internet-economy/tres-usos-del-blockchain-mas-alla-del-bitcoin-2869296

- **Caso 3[34]:** Davivienda y el BID: El grupo BID y Davivienda anuncia la emisión de un bono dentro de una BLOCKCHAIN en América Latina y el Caribe como un piloto acotado del SandBox[35] regulatorio de Colombia.

**Figura 10 Banco Davivienda**


Fuente: Forbes Colombia.

[34] Fuente: Forbes Colombia Davivienda y BID emiten el primer bono de blockchain en Colombia {página web} {en línea} {consultado el 21 de octubre 2023} Disponible en: https://forbes.co/2022/08/23/economia-y-finanzas/davivienda-y-el-bid-emiten-el-primer-bono-de-blockchain-en-colombia

[35] Fuente: CRCOM ¿Qué es un Sandbox regulatorio? {pagina web} {en línea} {consultado el 21 de octubre 2023} Disponible en: https://www.crcom.gov.co/es/preguntas-frecuentes/es-un-sandbox-regulatorio

- **Caso 4[36]:** Dos bancos Colombianos Davivienda y Banco de Bogotá, se integraron a la BLOCKCHAIN interbancaria de JPMorgan.

Un total de 37 bancos latinoamericanos participan en la red interbancaria basada en BLOCKCHAIN, desarrollada por la banca de inversión estadounidense JPMorgan Chase.

**Figura 11 Sucursal Banco de Bogotá**


Fuente: Forbes Colombia.

[36] Fuente: COLOMBIA Fintech, Dos bancos colombianos, Davivienda y Banco de Bogotá, se integraron a la blockchain interbancaria de JPMorgan {página web} {en línea} {consultado el 21 de octubre 2023} disponible en: https://colombiafintech.co/lineaDeTiempo/articulo/dos-bancos-colombianos-davivieda-y-banco-de-bogota-se-integraron-a-la-blockchain-interbancaria-de-jpmorgan

## 6.4 JUSTIFICAR MEDIANTE UN BREVE ANÁLISIS TÉCNICO, COMO LAS CRIPTOMONEDAS Y TOKENS PUEDE SER UTILIZADOS COMO MEDIO DE PAGO DESCENTRALIZADO, LAS CUALES SE APRECIAN DEPENDIENDO DE LA BLOCKCHAIN A LA QUE PERTENECEN

En este apartado, se simulará una BLOCKCHAIN utilizando Python[37], es un lenguaje de programación que es popular para el desarrollo de aplicaciones web, el desarrollo de software, la ciencia de datos y el machine learning. Es un lenguaje fácil de aprender y usar, y es compatible con muchas plataformas diferentes.

En esta sección, se simula una BLOCKCHAIN utilizando Python. Se crea una red de computadoras y se almacenan datos en la red. Luego, se probará la seguridad de la red simulando un ataque.

Se diseño un código que representa una simulación de una cadena de bloques, que es una forma de almacenar información de manera segura y confiable. Aquí hay una descripción básica de lo que hace el código:

Imagina que tienes una lista de bloques, y cada bloque contiene información. Cada bloque está vinculado al bloque anterior mediante un código llamado "hash". Un hash es como una huella digital única para cada bloque. Esto asegura que los bloques estén ordenados y conectados de manera segura.

El código comienza definiendo una estructura de bloque. Un bloque tiene un número, una marca de tiempo, información y un hash anterior. También tiene un "nonce" y un hash propio. Un nonce es un número aleatorio que se utiliza para crear un hash que cumpla con ciertos requisitos.

Luego, hay una función para generar un nuevo bloque. Esta función toma información como el número, la información y el hash anterior, y crea un nuevo bloque con una marca de tiempo actual.

Después, hay una función para "minar" un bloque. La minería es un proceso que requiere resolver un problema matemático complejo para encontrar un nonce que produzca un hash que cumpla con ciertos requisitos. Este proceso asegura que el bloque sea seguro. La función de minería intenta diferentes valores de nonce hasta encontrar uno que funcione.

Luego, el código crea el bloque "génesis", que es el primer bloque en la cadena. A partir de ahí, se simula la creación de nuevos bloques.

[37] Fuente: AWS ¿Qué es Python? {página web} {en línea} {consultado el 28 de junio 2023} disponible en: https://aws.amazon.com/es/what-is/python

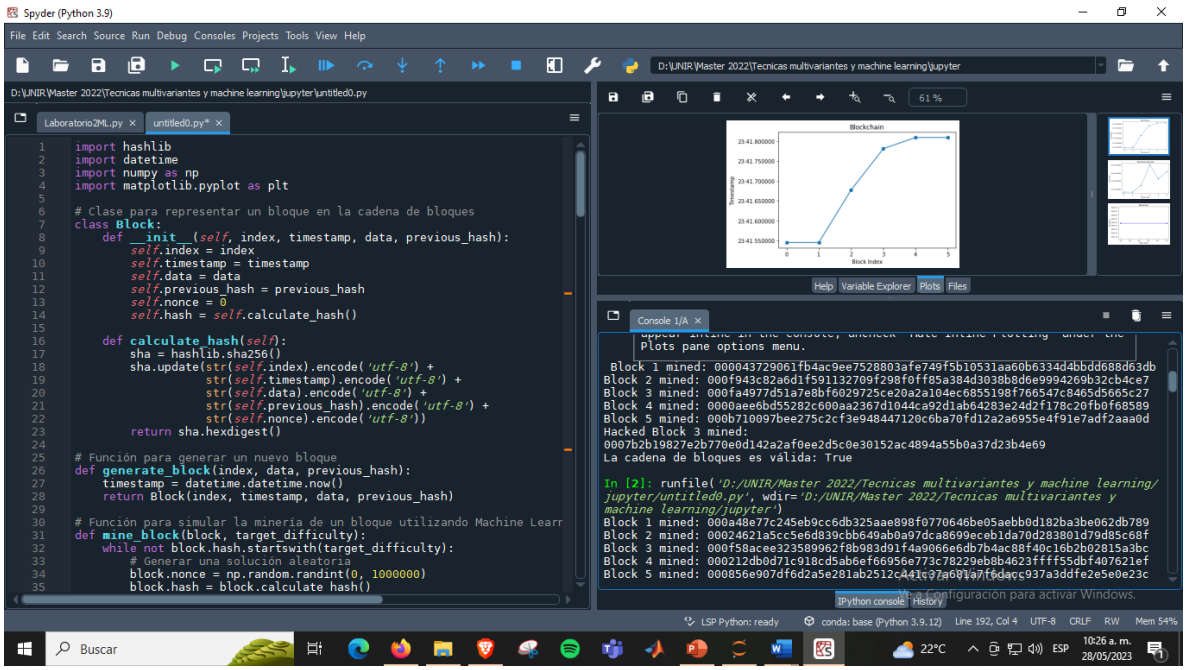
Finalmente, el código muestra una representación gráfica de la cadena de bloques utilizando una biblioteca llamada "matplotlib". Esto proporciona una visualización de los bloques y sus marcas de tiempo.

Este código muestra cómo se pueden crear y asegurar bloques en una cadena de bloques simulada. A través de la minería y la conexión segura entre los bloques, se puede garantizar la integridad de la información almacenada en la cadena de bloques.

En la figura 12 se representa como se minarían los bloques de una transacción mediante BLOCKCHAIN.

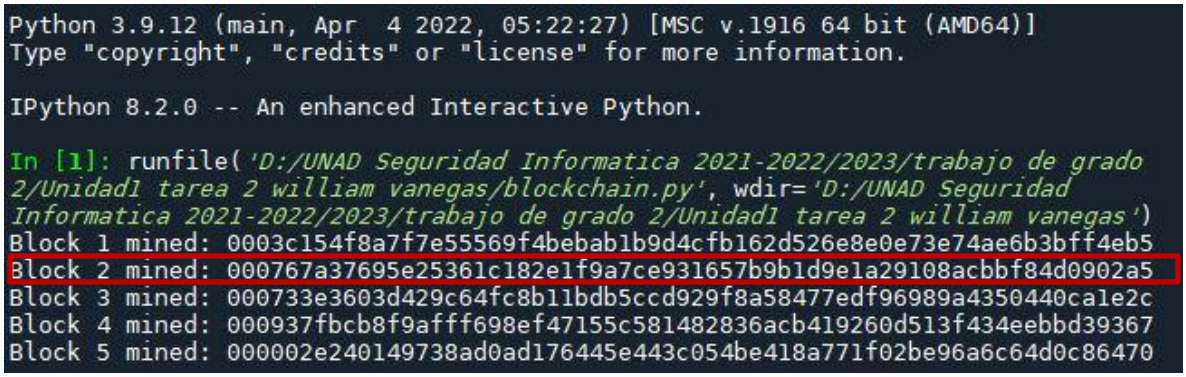
Posteriormente, en la figura 13 se muestran los códigos hash de los bloques simulados que en este caso son 5.

**Figura 12 Código simulación en Python de una blockchain**




Fuente: Elaboración Propia

**Figura 13 Bloques creados con sus respectivos códigos hash.**

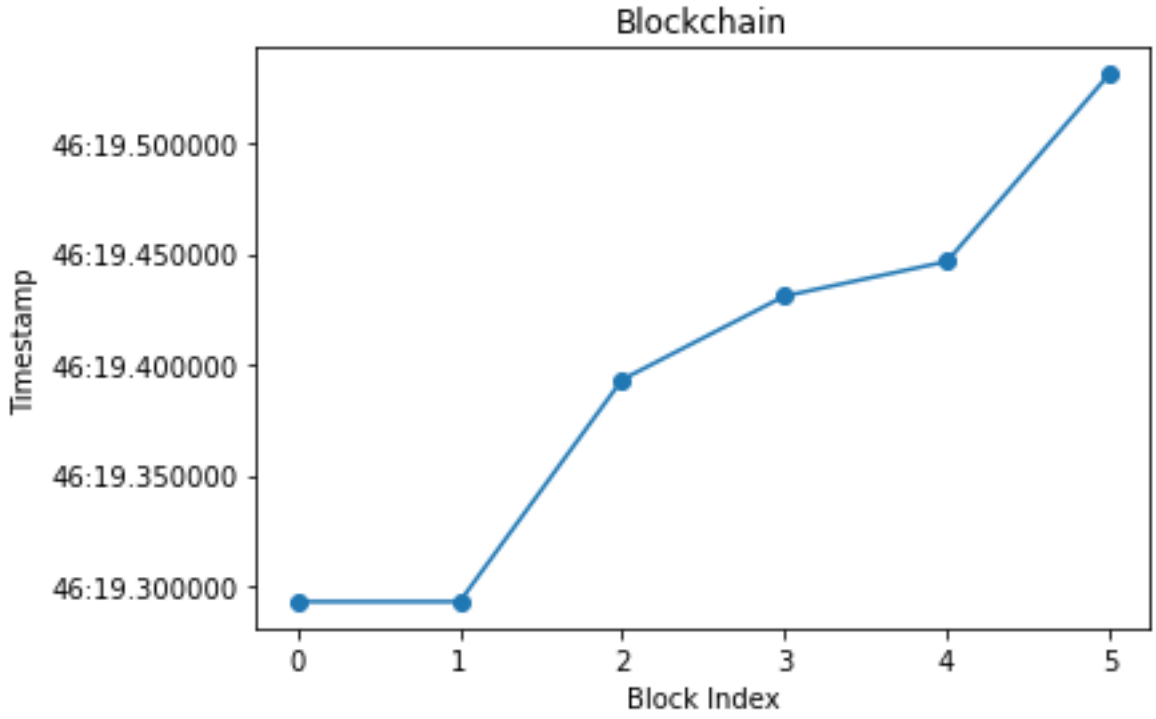



Fuente: Elaboración propia.

En este caso, todos los códigos hash son válidos, no han sido atacados, por lo tanto, los nodos validaran la transacción.

Se aprecia en la figura 14 gráficamente que, los códigos hash son validados por la simulación dejando pasar la transacción correctamente.

**Figura 14 Simulación de una transacción aprobada en una blockchain**




Luego se simula un ataque cibernético en el bloque 3 como se aprecia en la figura 15, el hash ha sido comprometido, los nodos deberán rechazar la transacción que se pretende enviar:

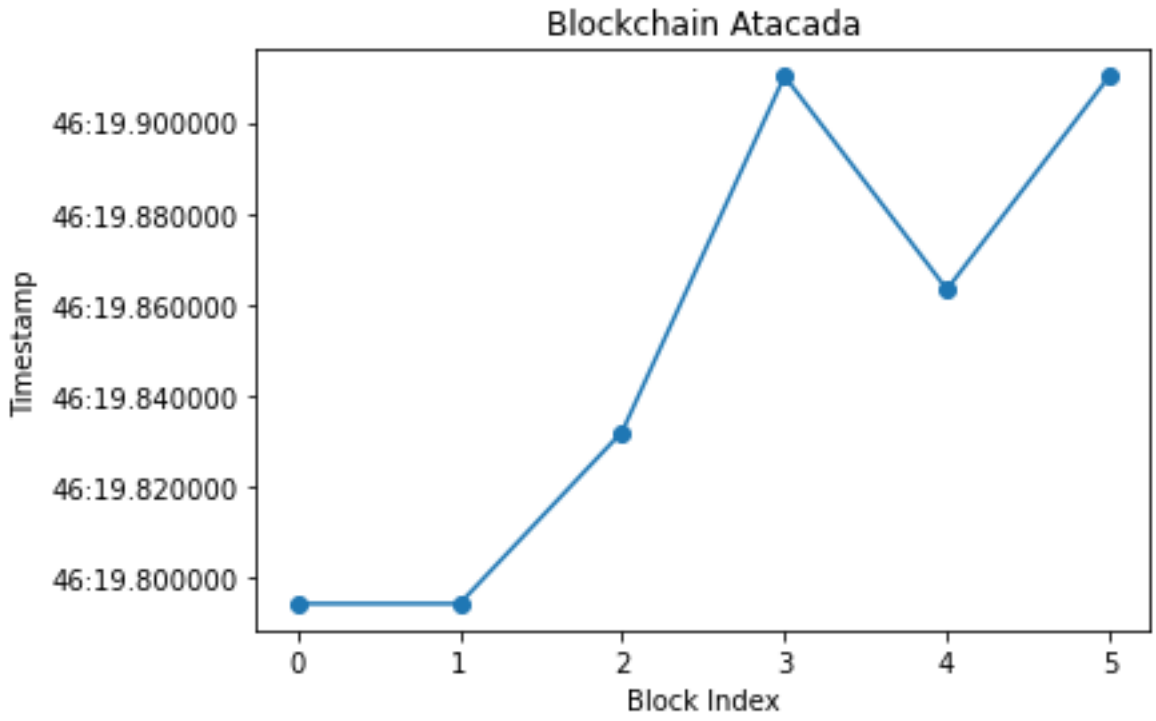
**Figura 15 Simulación de ataque al bloque 3 de una blockchain**

```
Block 1 mined: 0009fa9f67cfcdff625db97b4ee204f85a97ed787861d24053c08247a3869ee5
Block 2 mined: 0004083916feec9d3fa913d72068d8ab65887705b9a28c6bf14d22d23a150c41
Block 3 mined: 000635407228c2307d22d8db6c17990b67b85652992fb25b3c16e93d6738107d
Block 4 mined: 000bc850ed9c388b60ba759fa25a88bc618fbde861b41c001296bea83f9803fc
Block 5 mined: 000e149760dd6ee5a39962464bb9284641337cd3fe9ebf9f85426742bb75ddcf
Hacked Block 3 mined:
000fea9ce8a4908a2b1973667ea2bd5dbd01f4c720c8396a5ef4147fca7f6d6d
```

Fuente: Elaboración propia.

Se aprecia en la figura 16 gráficamente, el rechazo de este bloque ya que no es validado por la simulación.

**Figura 16 Bloque rechazado en la transacción de una blockchain**




En la gráfica, se puede apreciar que todos los bloques, excepto el bloque hackeado, siguen una progresión lineal en términos de timestamps. Esto indica que los bloques fueron generados de manera legítima y están en orden correcto.

Sin embargo, el bloque hackeado, que fue modificado intencionalmente, muestra una interrupción en la secuencia lineal. Esto indica que la cadena de bloques ha sido comprometida y se ha realizado un intento de alteración de datos.

Las gráficas muestran visualmente cómo los bloques de la cadena de bloques se van generando y cómo se produce una anomalía cuando se intenta un ataque de hackeo. Esto destaca la importancia de mantener la integridad y seguridad de la cadena de bloques para evitar modificaciones no autorizadas.

También, el análisis técnico en la negociación de criptoactivos, es un enfoque utilizado para evaluar los precios y los movimientos del mercado utilizando principalmente gráficos históricos y datos de volumen. Su objetivo es predecir las futuras tendencias de precios y aprovechar las oportunidades de trading en función de patrones pasados y comportamientos del mercado.

Los analistas técnicos creen que la acción del precio y los movimientos del mercado tienden a repetirse en patrones reconocibles. Utilizan herramientas y técnicas específicas, como líneas de tendencia, patrones de velas, indicadores técnicos y

análisis de volumen, para identificar estos patrones y tomar decisiones de trading fundamentadas.

Algunos conceptos clave en el análisis técnico incluyen:

**Líneas de tendencia:** Son líneas trazadas en un gráfico para conectar los puntos altos o bajos de los precios. Ayudan a identificar la dirección general de la tendencia y los posibles puntos de reversión.

**Patrones de velas**: Estos patrones se forman a partir de las velas en un gráfico y proporcionan señales sobre la posible dirección futura del precio. Ejemplos comunes de patrones de velas incluyen los patrones de reversión, como el martillo o el hombre colgado.

**Indicadores técnicos:** Son fórmulas matemáticas aplicadas a los datos del precio y el volumen para obtener información adicional sobre el comportamiento del mercado. Los indicadores técnicos populares incluyen el promedio móvil, el índice de fuerza relativa (RSI) y las bandas de Bollinger.

**Análisis de volumen:** El volumen es la cantidad de activos que se negocian en un determinado período de tiempo. El análisis de volumen ayuda a los analistas técnicos a evaluar la fuerza detrás de los movimientos del precio y confirmar las señales generadas por otros indicadores técnicos.

Es importante tener en cuenta que el análisis técnico se basa en la premisa de que el precio y los movimientos del mercado contienen toda la información necesaria para tomar decisiones de trading, sin tener en cuenta factores fundamentales o noticias externas. Sin embargo, muchos traders combinan el análisis técnico con el análisis fundamental para obtener una visión más completa del mercado.

En el contexto colombiano, es posible adquirir y comercializar criptomonedas a través de plataformas especializadas conocidas como exchanges. Un ejemplo de un exchange popular es Binance, el cual ha establecido una alianza con la entidad bancaria Davivienda.

Binance ofrece a los usuarios la posibilidad de realizar transacciones peer-to-peer (p2p), es decir, transacciones directas entre personas. Estas transacciones se llevan a cabo en la plataforma y cuentan con validación y certificación previa, lo que brinda garantías sobre la legalidad y legitimidad del dinero invertido.

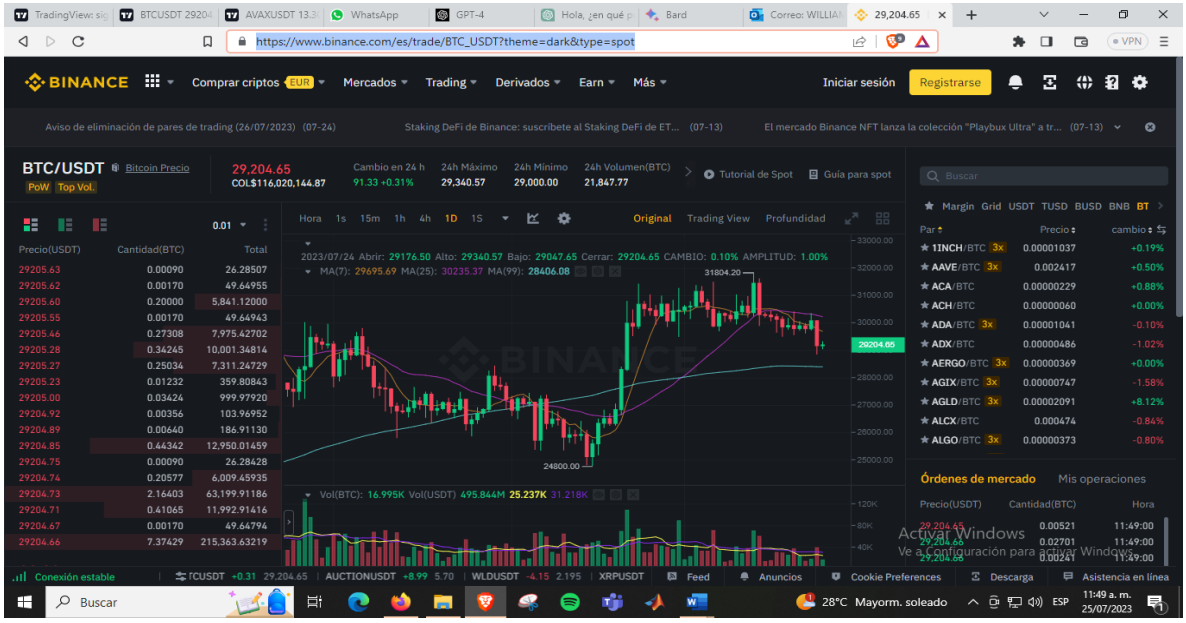
Además, Binance facilita la compra de criptomonedas utilizando diversos medios de pago, como tarjetas de crédito y débito. Esto brinda a los usuarios una amplia flexibilidad para adquirir criptomonedas de forma conveniente y segura.

Es importante destacar que, al utilizar plataformas de intercambio de criptomonedas, como Binance, los usuarios deben seguir las normativas y regulaciones locales relacionadas con el comercio de activos digitales.
Esto incluye cumplir con los requisitos de identificación y verificación establecidos por la plataforma y las autoridades regulatorias correspondientes.

En resumen, en Colombia es posible adquirir y comerciar criptomonedas a través de plataformas especializadas[38] como Binance, que ofrece opciones de transacciones p2p y diversas formas de pago. Sin embargo, es fundamental que los usuarios cumplan con las regulaciones locales y realicen sus transacciones de manera responsable y segura.

En la figura 20, se representa la plataforma de intercambio Binance y el par BTC/USDT.

**Figura 17 Exchange de criptomonedas Binance**




Fuente: https://www.binance.com/es/trade/BTC_USDT?theme=dark&type=spot

En la ilustración anterior, se puede apreciar el valor que ha adquirido bitcoin desde que fue enlistada en Binance[39], esto da a entender que la BLOBKCHAIN es muy robusta segura y confiable.

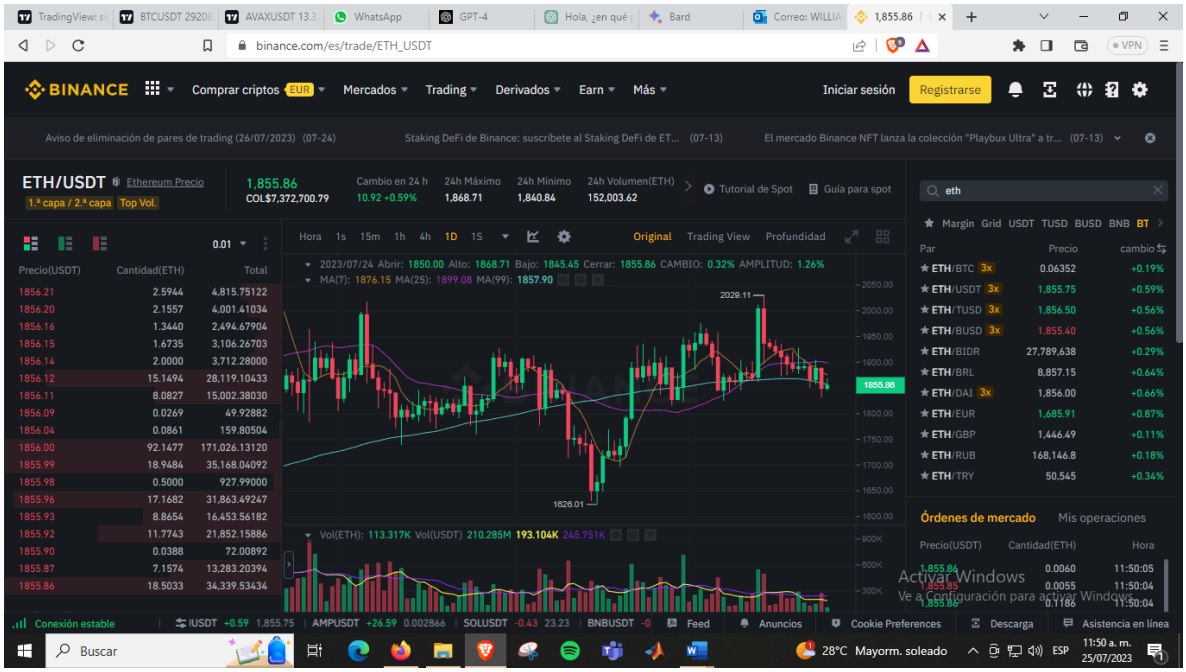
[38] Fuente: LA REPUBLICA Binance y Davivienda formaron una de las nueve alianzas que probaran criptoactivos {1 marzo 2021} {en línea} {consultado el 27 de junio 2023} disponible en: https://www.larepublica.co/finanzas/binance-y-davivienda-formaron-una-de-las-nueve-alianzas-que-probaran-criptoactivos-3132002
[39] Fuente: BINANCE {página web} {en línea} {consultado el 28 de mayo 2023} disponible en: https://www.binance.com/

También se debe tener en cuenta que existen criptomonedas denominadas stablecoins[40], las cuales van ancladas al precio del dollar o euro según el caso, esto las convierte en un activo ideal para realizar transacciones evitando la volatilidad. La criptomoneda que en este caso es BTC, se puede vender al precio del dólar convirtiéndola en USDT (dólar theter).

Si se desea, se puede adquirir BTC teniendo USDT que tiene un valor de 29.247 dls, pero es posible adquirir fracciones de BTC o de cualquier criptomoneda disponible, no obligatorio la compra total del criptoactivo.

En la figura 18, se representa el comportamiento de la criptomoneda ETH/USDT.

**Figura 18 Precio de ETH en el exchange Binance**




Fuente: https://www.binance.com/es/trade/ETH_USDT

Al igual que el caso anterior con BTC, se puede apreciar que la BLOCKCHAIN publica Ethereum, ha adquirido bastante funcionalidad, también teniendo en cuenta la línea azul, se aprecia que su tendencia posiblemente sea al alza en los próximos meses. Se debe tener en cuenta que, estos análisis son totalmente especulativos y no dan una certeza real del precio de un activo, por lo que son considerados inversiones de alto riesgo por lo que son susceptibles a manipulaciones.

[40] Stablecoins: Monedas ancladas al dinero FIAT algunas de ellas son USDT, DAI, BUSD, EURO entre otras.

### 6.4.1 Criptomonedas o tokens como medio de pago

Las criptomonedas o tokens son un tipo de activo digital que se basa en la tecnología BLOCKCHIAN. Esta tecnología permite registrar transacciones de forma segura y transparente, lo que las hace ideales para su uso como medio de pago.

Las criptomonedas se pueden utilizar como medio de pago de la misma manera que las monedas fiduciarias, como el dólar estadounidense o el euro. Los usuarios pueden enviar y recibir criptomonedas entre sí, y pueden utilizarlas para comprar bienes y servicios.

Ventajas de las criptomonedas como medio de pago:

- Transacciones seguras y transparentes: Las transacciones con criptomonedas se registran en la BLOCKCHAIN, lo que las hace muy seguras y transparentes.

- Costos de transacción bajos: Los costos de transacción con criptomonedas suelen ser mucho más bajos que los costos de transacción con monedas fiduciarias.

- Transacciones internacionales: Las criptomonedas se pueden utilizar para realizar transacciones internacionales de forma rápida y eficiente.

Monedas estables[41]:

Las monedas estables son un tipo de criptomoneda que está diseñada para mantener su valor estable en relación con una moneda fiduciaria, como el dólar estadounidense. Esto las hace ideales para su uso como medio de pago, ya que eliminan la volatilidad de las criptomonedas tradicionales.

Beneficios de las monedas estables como medio de pago:

- Menor volatilidad: Las monedas estables tienen una volatilidad mucho menor que las criptomonedas tradicionales, lo que las hace más atractivas para los comerciantes y los consumidores.

- Aceptación más amplia: Las monedas estables suelen ser aceptadas por una gama más amplia de comerciantes que las criptomonedas tradicionales.

[41] Fuente: BUDA Stablecoin: ¿Qué es? {pagina web} {en línea} {consultado el 24 de octubre 2023} disponible en: https://www.buda.com/guias/stablecoin

Las criptomonedas y los tokens tienen el potencial de revolucionar el comercio electrónico. La tecnología BLOCKCHAIN permite realizar transacciones de forma segura, transparente y eficiente, lo que ofrece a los comerciantes y los consumidores una serie de ventajas.

Las monedas estables son una variante de las criptomonedas que ofrecen un mayor atractivo para los comerciantes y los consumidores, ya que tienen una menor volatilidad y una aceptación más amplia.

Algunas de las más conocidas son USDT, USDC, DAI las cuales pueden utilizar cualquier tipo de BLOCKCHAIN para realizar transacciones y conservan paridad con el dólar estadounidense.

Colombia está avanzando en la creación de una moneda digital[42], utilizando la BLOCKCHAIN ripple, la cual en este momento se encuentra en fase de desarrollo junto con el MINTIC y el Banco de la República, la cual tendrá paridad con el peso colombiano.

Esta moneda digital, será regulada por el gobierno, por lo que se evitaría al máximo algún tipo de fraude y las transacciones serán más rápidas y económicas.

**Figura 19 moneda digital colombiana**

Fuente: INFOBAE: https://www.infobae.com/colombia/2023/06/21/banco-de-la-republica-y-mintic-firman-importante-acuerdo-para-crear-moneda-central-digital/

[42] Fuente: INFOBAE Crearan una moneda digital en Colombia: en que consiste el acuerdo entre el banco de la republica y el ministerio de las TIC. {pagina web} {en línea} {consultado el 24 de octubre 2023} disponible en: https://www.infobae.com/colombia/2023/06/21/banco-de-la-republica-y-mintic-firman-importante-acuerdo-para-crear-moneda-central-digital/

# 7 CONCLUSIONES

- El protocolo PoA es la mejor opción para la protección de transacciones financieras en Colombia, ya que ofrece un equilibrio óptimo entre seguridad, eficiencia y descentralización. PoA es más seguro que otros protocolos, como PoW y PoS, ya que no requiere que los nodos resuelvan algoritmos criptográficos complejos. Esto lo hace más eficiente en términos de consumo de energía y costos. Además, PoA es más descentralizado que otros protocolos, ya que no requiere que los nodos tengan que invertir en hardware especializado, además la normativa ISO 20022 versión 2019 también es un factor importante para la seguridad de las transacciones financieras en Colombia. Esta normativa proporciona directrices y mejores prácticas para la implementación de sistemas basados en BLOCKCHAIN, asegurando la interoperabilidad, la seguridad y la confidencialidad de los datos.

- La adopción de la tecnología BLOCKCHAIN en el sistema financiero colombiano tendría un impacto positivo significativo en términos de eficiencia, transparencia, seguridad y confianza. En cuanto a la eficiencia, esta tecnología podría reducir los tiempos de procesamiento de pagos y eliminar intermediarios costosos, mejorando la eficiencia en las transacciones financieras y reduciendo los costos para consumidores y empresas. Además, en términos de transparencia, proporcionaría un registro mucho más confiable, ayudando a prevenir fraudes y aumentar la confianza en el sistema financiero. En cuanto a la seguridad, la BLOCKCHAIN ofrecería una mayor protección contra fraudes y garantizaría una gestión más confiable de los activos financieros, contribuyendo así a mejorar la seguridad financiera en Colombia, sin embargo, es importante destacar que la implementación efectiva de esta tecnología requiere la colaboración y participación de diferentes actores, así como la consideración de aspectos clave como la interoperabilidad entre sistemas existentes, la seguridad cibernética y la capacitación adecuada de los profesionales. Con estos elementos en su lugar, la adopción de la BLOCKCHAIN podría ofrecer un impulso significativo a la eficiencia y la confianza en el sistema financiero colombiano.

- Las transacciones de tokens o criptoactivos en una BLOCKCHAIN representan un avance significativo en la forma en que se llevan a cabo las operaciones financieras. Esta tecnología no solo mejora la seguridad y la transparencia, sino que también ofrece la posibilidad de una mayor eficiencia, reducción de costos y accesibilidad global. A medida que continúa evolucionando, la BLOCKCHAIN tiene el potencial de cambiar fundamentalmente la forma en que interactuamos con los activos y las transacciones en la economía global.

# 8 RECOMENDACIONES

- Se recomienda realizar un análisis exhaustivo de los requisitos y necesidades del comercio electrónico antes de seleccionar el tipo de BLOCKCHAIN a implementar, por lo que es importante evaluar cuidadosamente las características y capacidades de cada tipo de BLOCKCHAIN para asegurarse de que se ajuste adecuadamente a los requisitos de seguridad y gestión de datos sensibles en transacciones financieras.

- La tecnología BLOCKCHAIN es altamente recomendable para cualquier empresa o entidad que desee mejorar sus índices de seguridad en transacciones financieras, contratos inteligentes, custodia de archivos, entre muchas otras, incluso si desea obtener algún derecho de autor de una obra de arte, es posible con esta tecnología, ya que el código que se genera es único para cada autor (NFT)[43].

- El consumo energético es un factor importante por considerar al seleccionar un protocolo de validación de bloques. Los protocolos de consenso basados en prueba de trabajo (PoW) son los más intensivos en energía, ya que requieren que los nodos de la red resuelvan complejos problemas matemáticos para validar las transacciones. Los protocolos basados en prueba de participación (PoS) y prueba de autoridad (PoA) son más eficientes en energía, ya que no requieren que los nodos resuelvan problemas matemáticos.

- La seguridad es otro factor importante al seleccionar un protocolo de validación de bloques. Los protocolos de consenso basados en PoW son los más seguros, ya que son muy difíciles de manipular. Los protocolos basados en PoS y PoA son menos seguros que PoW, pero aún son muy seguros.

- La escalabilidad es importante tenerla en cuenta al seleccionar un protocolo de validación de bloques. Los protocolos de consenso basados en PoW son los menos escalables, ya que se vuelven más lentos y costosos a medida que aumenta el número de transacciones. Los protocolos basados en PoS y PoA son más escalables que PoW, pero aún tienen limitaciones.

[43] Token no fungible validado por una BLOCKCHAIN especializada en el manejo de activos como obras de arte, musicales, videojuegos, etc.

# 9 DIVULGACIÓN

El desarrollo del presente proyecto de grado será dado a conocer en colaboración de la biblioteca de la Universidad Nacional Abierta y a Distancia – UNAD, a través de su aplicativo en línea, en donde se publicará un archivo PDF correspondiente al documento final presentado ante los jurados, posterior a la sustentación de este (Si es informe técnico por seminario o créditos de maestría, no tiene jurado); con el fin de que todos los estudiantes de la Universidad que se encuentren interesados en el tema de la tecnología BLOCKCHAIN y su implementación como validador de transacciones financieras en el comercio electrónico de Colombia , puedan acceder al documento.

## BIBLIOGRAFÍA

ADOPCIÓN DE LA TECNOLOGÍA BLOCKCHAIN EN EL SECTOR FINANCIERO COLOMBIANO LUZ ADRIANA PINO RIVERA ALFREDO PRADO HERNÁNDEZ - PDF Descargar libre {Anónimo}. Le proporcionamos las herramientas cómodas y gratuitas para publicar y compartir la información. {página web}. {Consultado el 19, octubre, 2023}. Disponible en Internet: https://docplayer.es/168999785-Adopcion-de-la-tecnologia-blockchain-en-el-sector-financiero-colombiano-luz-adriana-pino-rivera-alfredo-prado-hernandez.html .

Bitcoin - Open source P2P money {página web}. {Consultado el 20, octubre, 2023}. Disponible en Internet: https://bitcoin.org/bitcoin.pdf .

CABALLERO, Jhon. Criptomonedas, Blockchain Y Contratos Inteligentes Universidad Externado de Colombia 2019 disponible en: https://bdigital.uexternado.edu.co/handle/001/2592 CAMPOS, Freddy. Las Criptomonedas Y La Internet Del Dinero. 2018 debates IESA, 23(2), 6–8. disponible en: http://search-ebscohost-com.luisamigo.proxybk.com/login.aspx?direct=true&db=asn&AN=138021192&lang=es&site=ehost-live%0A%0A%0A

ESPINOSA, Sergio.Guía de referencia de Blockchain para la adopción e implementación de proyectos en el Estado Colombiano. *MinTIC*, {Consultado el 20 de octubre 2023}. Disponible en: https://www.arduino.cc/reference/es/

ETHEREUM WHITEPAPER | ethereum.org {página web}. {Consultado el 19, diciembre, 2023}. Disponible en Internet: https://ethereum.org/en/whitepaper .

FERNANDEZ Alonso. Criptomonedas en tiempos de pandemia: ¿hacia la precipitación de un nuevo orden monetario internacional? Temas y Debates, 2021 449–456. disponible en: https://doi.org/10.35305/tyd.v0i0.521

GARCIA, Bryan. Herramienta web con tecnología de cadena de bloques para un sistema de facturación electrónica en Colombia. *Información Tecnológica*, *32*(3), 2021 15–24 disponible en: https://doi.org/10.4067/s0718-07642021000300015

GOMEZ, Eugenio., & CAZARES, Verónica. *Bitcoin Todo lo que hay que saber*.2019 51.

GOULD Rick, BANNABY Lewis, LOCKETT Kath, La nueva ola en finanzas {en línea} {enero 2020} {consultado el 25 de julio 2023} disponible en:

https://www.iso.org/files/live/sites/isoorg/files/news/magazine/ISOfocus%20(2013-NOW)/sp/ISOfocus_138_sp.pdf

GÜRFIDAN, Remzy., ERSOY, Melvüt. Blockchain-based music wallet for copyright protection in audio files. Journal of Computer Science and Technology (Argentina), 2021 *21*(1), 11–19. disponible en:https://doi.org/10.24215/16666038.21.E2

HILEMAN Garrick, RAUCHS Michel {Sitio web} {en línea} GLOBAL BLOCKCHAIN BENCHMARKING STUDY UNIVERSITY OF CAMBRIDGE {Consultado el 25 de julio 2023} disponible en: https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2017-09-27-ccaf-globalbchain.pdf

LA TECNOLOGÍA Blockchain en la construcción de espacios económicos de impacto social positivo | REVESCO. Revista de Estudios Cooperativos {Anónimo}. Home Page {página web}. {Consultado el 19, diciembre, 2023}. Disponible en Internet: https://doi.org/10.5209/REVE.73867 .

LUCIANO BENITEZ, Romulo. de S. (2018). Aplicação da Smart Contract nos Contratos de Gás Natural: Uma Análise Exploratória. Revista de Administração Contemporânea,2018 22(6), 903–921. disponible en: https://doi.org/10.1590/1982-7849rac2018180136

MALDONADO Jose, Quien es W Scott Stornetta? Bit2me Academia {pagina web} {en linea} {consultado el 24 de julio 2023} disponible en: https://academy.bit2me.com/quien-es-w-scott-stornetta/

MARESME, Mataro. Blockchain y su impacto en la industria de la ciberseguridad 2021 disponible en: https://www.esedsl.com/blog/blockchain-impacto-industria-ciberseguridad

MARR Bernard, Estas son las cinco mayores tendencias de blockchain para 2022 revista Forbes {Pagina web} {en línea} {consultado el 24 de julio 2023} disponible en https://forbes.es/criptomonedas/126653/estas-son-las-cinco-mayores-tendencias-de-blockchain-en-2022/

MINTIC Guía de referencia de blockchain para la adopción e implementación de proyectos en el estado colombiano {en línea} {Consultada el 25 de mayo 2023} disponible en: https://gobiernodigital.mintic.gov.co/692/articles-161810_pdf.pdf

MORGAN, J. ISO 20022 El lenguaje universal para el futuro de pagos {en línea} {Consultada el 17 de junio de 2023} disponible en: https://www.jpmorgan.com/content/dam/jpm/global/documents/iso-20022-spanish-white-paper-ada-compliant.pdf

MUÑOZ Aitor, Sistema de Verificación de documentos usando arboles de Merkle,{en línea} Grado de ingeniería informática, Madrid España, Universidad Autónoma de Madrid, Escuela politécnica superior 2018 51p{consultado el 24 de julio 2023}.Disponible en: https://repositorio.uam.es/bitstream/handle/10486/688980/mu%c3%b1oz_cu%c3%b1a_aitor_tfg.pdf?sequence=1&isAllowed=y

NATURALEZA JURÍDICA de las criptomonedas a la luz de los pronunciamientos de soft law en Colombia | Revista Jurídica Piélagus {Anónimo}. Home Page {página web}. {Consultado el 19, diciembre, 2023}. Disponible en Internet: https://doi.org/10.25054/16576799.2822 .

ODDONE, Jorge.Aplicación de blockchain y smart contracts en la compraventa de vehículos usados 194-208.

PACHECO Jiménez. De la tecnología blockchain a la economía del token. Derecho PUCP,2019 83, 61–87 disponible en: https://doi.org/10.18800/derechopucp.201902.003

SAMANIEGO, Juan. La tecnología blockchain en la industria 4.0: casos y aplicaciones. Hablemos de Empresas 2018 Disponible en: https://hablemosdeempresas.com/grandes-empresas/blockchain-en-la-industria/

SANCHEZ, Moreno. ¿Cuándo llegará la regulación de las criptomonedas? 2021 especial Directivos, 1793, 25–29.

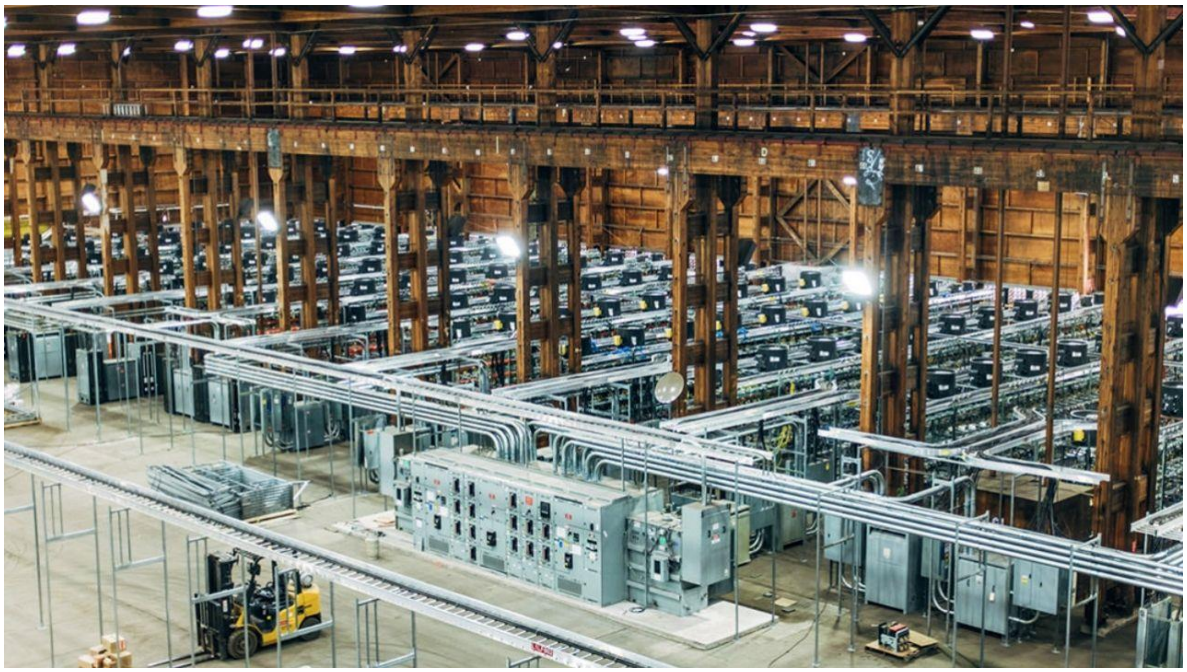
TASENDE, I. Blockchain y arbitraje: un nuevo enfoque en la resolución de disputas. Especial énfasis en smartcontracts y criptodivisas. *Revista de Derecho*, *22*(22), 2020 138–159. disponible en: https://doi.org/10.22235/rd22.2127

VISTA DE Blockchain: una revolución de vieja data [Anónimo]. Portal de revistas {página web}. {Consultado el 19, octubre, 2023}. Disponible en Internet: https://revistas.bibdigital.uccor.edu.ar/index.php/rbia/article/view/5152/3649 .

# ANEXOS

**Anexo A Nodo Validador**

**Figura 20 Granja minería bitcoin ubicada en la Plata Argentina**



Fuente: https://runrunelectrico.com/empezo-a-construirse-la-granja-de-bitcoins-mas-grande-de-argentina/

**Anexo B** Uso de energía volcánica para minado de bitcoin en El Salvador
https://forbes.co/2021/09/29/actualidad/videos-el-salvador-comenzo-a-minar-bitcoin-con-energia-geotermica-de-sus-volcanes/

**Anexo C Código en Python simulación de BLOCKCHAIN**

```
import hashlib
import datetime
import numpy as np
import matplotlib.pyplot as plt

# Clase para representar un bloque en la cadena de bloques
class Block:
    def __init__(self, index, timestamp, data, previous_hash):
        self.index = index
        self.timestamp = timestamp
        self.data = data
        self.previous_hash = previous_hash
        self.nonce = 0
        self.hash = self.calculate_hash()

    def calculate_hash(self):
        sha = hashlib.sha256()
        sha.update(str(self.index).encode('utf-8') +
                   str(self.timestamp).encode('utf-8') +
                   str(self.data).encode('utf-8') +
                   str(self.previous_hash).encode('utf-8') +
                   str(self.nonce).encode('utf-8'))
        return sha.hexdigest()

# Función para generar un nuevo bloque
def generate_block(index, data, previous_hash):
    timestamp = datetime.datetime.now()
    return Block(index, timestamp, data, previous_hash)

# Función para simular la minería de un bloque utilizando Machine Learning
def mine_block(block, target_difficulty):
    while not block.hash.startswith(target_difficulty):
        # Generar una solución aleatoria
        block.nonce = np.random.randint(0, 1000000)
        block.hash = block.calculate_hash()

# Configuración inicial
difficulty = 3  # Dificultad objetivo
genesis_block = generate_block(0, 'Genesis Block', '0')
blockchain = [genesis_block]

# Simulación de la creación de nuevos bloques
for i in range(1, 6):
```

```
    previous_block = blockchain[-1]
    new_block = generate_block(i, f'Data for Block {i}', previous_block.hash)

    # Simulación del proceso de minería utilizando Machine Learning
    mine_block(new_block, '0' * difficulty)

    blockchain.append(new_block)
    print(f'Block {new_block.index} mined: {new_block.hash}')

# Obtener los valores para la representación gráfica
block_indices = [block.index for block in blockchain]
block_timestamps = [block.timestamp for block in blockchain]

# Crear la figura y los ejes
fig, ax = plt.subplots()
ax.plot(block_indices, block_timestamps, 'o-')

# Configurar el eje x
ax.set_xlabel('Block Index')

# Configurar el eje y
ax.set_ylabel('Timestamp')

# Configurar el título del gráfico
ax.set_title('Blockchain')

# Mostrar el gráfico
plt.show()

# Clase para representar un bloque en la cadena de bloques
class Block:
    def __init__(self, index, timestamp, data, previous_hash):
        self.index = index
        self.timestamp = timestamp
        self.data = data
        self.previous_hash = previous_hash
        self.nonce = 0
        self.hash = self.calculate_hash()

    def calculate_hash(self):
        sha = hashlib.sha256()
        sha.update(str(self.index).encode('utf-8') +
                   str(self.timestamp).encode('utf-8') +
                   str(self.data).encode('utf-8') +
                   str(self.previous_hash).encode('utf-8') +
```

```
                str(self.nonce).encode('utf-8'))
        return sha.hexdigest()

# Función para generar un nuevo bloque
def generate_block(index, data, previous_hash):
    timestamp = datetime.datetime.now()
    return Block(index, timestamp, data, previous_hash)

# Función para simular la minería de un bloque utilizando Machine Learning
def mine_block(block, target_difficulty):
    while not block.hash.startswith(target_difficulty):
        # Generar una solución aleatoria
        block.nonce = np.random.randint(0, 1000000)
        block.hash = block.calculate_hash()

# Configuración inicial
difficulty = 3  # Dificultad objetivo
genesis_block = generate_block(0, 'Genesis Block', '0')
blockchain = [genesis_block]

# Simulación de la creación de nuevos bloques
for i in range(1, 6):
    previous_block = blockchain[-1]
    new_block = generate_block(i, f'Data for Block {i}', previous_block.hash)

    # Simulación del proceso de minería utilizando Machine Learning
    mine_block(new_block, '0' * difficulty)

    blockchain.append(new_block)
    print(f'Block {new_block.index} mined: {new_block.hash}')

# Intento de hackeo
hacked_block_index = 3
hacked_data = 'Hacked Data'
hacked_block = generate_block(hacked_block_index, hacked_data,
blockchain[hacked_block_index - 1].hash)

# Modificar el bloque hackeado
hacked_block.data = 'Modified Data'

# Reintentar la minería del bloque hackeado
mine_block(hacked_block, '0' * difficulty)

# Actualizar el bloque hackeado en la cadena de bloques
blockchain[hacked_block_index] = hacked_block
```

```
print(f'Hacked Block {hacked_block.index} mined: {hacked_block.hash}')

# Obtener los valores para la representación gráfica
block_indices = [block.index for block in blockchain]
block_timestamps = [block.timestamp for block in blockchain]

# Crear la figura y los ejes
fig, ax = plt.subplots()
ax.plot(block_indices, block_timestamps, 'o-')

# Configurar el eje x
ax.set_xlabel('Block Index')

# Configurar el eje y
ax.set_ylabel('Timestamp')

# Configurar el título del gráfico
ax.set_title('Blockchain Atacada')

# Mostrar el gráfico
plt.show()

class Block:
    def __init__(self, index, previous_hash, timestamp, data):
        self.index = index
        self.previous_hash = previous_hash
        self.timestamp = timestamp
        self.data = data
        self.hash = self.calculate_hash()

    def calculate_hash(self):
        hash_string = str(self.index) + str(self.previous_hash) + str(self.timestamp) +
str(self.data)
        return hashlib.sha256(hash_string.encode()).hexdigest()

class Blockchain:
    def __init__(self):
        self.chain = []
        self.timestamps = []

    def add_block(self, block):
        self.chain.append(block)
        self.timestamps.append(block.timestamp)

    def is_valid(self):
```

```
        for i in range(1, len(self.chain)):
            current_block = self.chain[i]
            previous_block = self.chain[i - 1]

            if current_block.hash != current_block.calculate_hash():
                return False

            if current_block.previous_hash != previous_block.hash:
                return False

        return True

    def plot_chain(self):
        block_indices = [block.index for block in self.chain]
        plt.plot(block_indices, self.timestamps, 'bo-')
        plt.xlabel('Block Index')
        plt.ylabel('Timestamp')
        plt.title('Blockchain')
        plt.show()

# Crear la cadena de bloques
blockchain = Blockchain()

# Crear bloque génesis
genesis_block = Block(0, "", datetime.datetime.now(), "Bloque Génesis")
blockchain.add_block(genesis_block)

# Crear bloque válido
block1 = Block(1, genesis_block.hash, datetime.datetime.now(), "Datos del bloque
1")
blockchain.add_block(block1)

# Crear bloque atacado (modificado intencionalmente)
block_attack = Block(2, block1.hash, datetime.datetime.now(), "Datos
modificados")
block_attack.timestamp += datetime.timedelta(minutes=10)  # Modificar el
timestamp para simular un ataque
# No se agrega el bloque atacado a la cadena de bloques

# Agregar el bloque atacado a la cadena de bloques (para simular un ataque
exitoso)
blockchain.add_block(block_attack)

# Verificar la validez de la cadena de bloques
print("La cadena de bloques es válida:", blockchain.is_valid())
```

```
# Graficar la cadena de bloques
blockchain.plot_chain()
```

**Estructura del documento para la estructura del Resumen Analítica Especializado -RAE**

| | |
|---|---|
| **Fecha de Realización:** | **20/10/2023** |
| **Programa:** | **Especialización en seguridad informática** |
| **Línea de Investigación:** | Gestión de Sistemas |
| **Título:** | LA TECNOLOGÍA BLOCKCHAIN Y SU IMPLEMENTACIÓN COMO VALIDADOR DE TRANSACCIONES FINANCIERAS EN EL COMERCIO ELECTRÓNICO DE COLOMBIA |
| **Autor(es):** | Vanegas Rodriguez William Edison |
| **Palabras Claves:** | BLOCKCHAIN, Smartcontracts, Criptomonedas, Minería de datos |
| **Descripción:** | En este documento, se explicó como la tecnología BLOCKCHAIN, por su naturaleza de funcionamiento, puede proteger de una manera muy efectiva, datos sensibles como financieros, documentación privada, e incluso secretos industriales, los cuales pueden verse amenazados por un ciberataque y la entidad o nosotros como individuos podríamos ser víctimas de algún hecho delictivo entre ellos estafas, extorsión, robo de información, entre otros. |

**Fuentes bibliográficas destacadas:**

AYALA ARISTIZABAL, Álvaro. Naturaleza jurídica de las criptomonedas a la luz de los pronunciamientos de soft law en Colombia. Revista Jurídica Piélagus, 2021 20(1), 19. disponible en: https://doi.org/10.25054/16576799.2822

ESPINOSA, Sergio. (2020). Guía de referencia de BLOCKCHAIN para la adopción e implementación de proyectos en el Estado Colombiano. *MinTIC*, 118. https://www.arduino.cc/reference/es/

FERNANDEZ Alonso. Criptomonedas en tiempos de pandemia: ¿hacia la precipitación de un nuevo orden monetario internacional? Temas y

Debates, 2021 449–456. disponible en: https://doi.org/10.35305/tyd.v0i0.521

GARCIA, Bryan. Herramienta web con tecnología de cadena de bloques para un sistema de facturación electrónica en Colombia. *Información Tecnológica*, *32*(3), 2021 15–24 disponible en: https://doi.org/10.4067/s0718-07642021000300015

| | |
|---|---|
| **Contenido del documento:** | El propósito fundamental de este documento es resaltar cómo la tecnología BLOCKCHAIN ofrece una confianza sólida en el ámbito del comercio electrónico, convirtiéndolo prácticamente en una fortaleza invulnerable frente a potenciales ataques cibernéticos.<br><br>La BLOCKCHAIN se ha erigido como una herramienta poderosa para la validación de transacciones de diversa índole, e incluso se están explorando sus posibilidades para mejorar la seguridad en el ámbito de la inteligencia artificial.<br><br>Esta tecnología adquirió una relevancia significativa a partir del año 2008, coincidiendo con la introducción de la criptomoneda bitcoin. La creación de esta nueva forma de intercambio de bienes y servicios, atribuida posiblemente a una figura enigmática o a un grupo de programadores conocidos como Satoshi Nakamoto, marcó un hito en la historia financiera y tecnológica.<br><br>Además, en el contexto colombiano, el comercio electrónico ha experimentado un crecimiento acelerado, impulsado en gran medida por la pandemia de COVID-19. Sin embargo, este crecimiento también ha revelado una serie de desafíos, tales como retrasos en las transacciones, entregas que no coinciden con los productos solicitados y, lamentablemente, estafas de gran envergadura. Aquí es donde la BLOCKCHAIN |

| | |
|---|---|
| | emerge como una solución capaz de mitigar estas deficiencias en materia de seguridad informática.<br><br>Este documento explorará detalladamente cómo la BLOCKCHAIN puede ofrecer una solución sólida y eficaz para mejorar la seguridad y la confiabilidad en el entorno del comercio electrónico, particularmente en el contexto colombiano, donde la necesidad de soluciones robustas es más evidente que nunca. |
| **Marco Metodológico:** | **Tipo de Investigación:** Este trabajo se basará en una investigación exploratoria y descriptiva. La exploratoria permitirá comprender la tecnología BLOCKCHAIN y sus aplicaciones, mientras que la descriptiva se enfocará en analizar casos de éxito y comparar protocolos.<br><br>**Enfoque Metodológico:** Se utilizará un enfoque cualitativo para comprender la aplicación práctica de la tecnología BLOCKCHAIN en transacciones financieras y un enfoque cuantitativo para comparar los protocolos de prueba de trabajo y prueba de participación.<br><br>Población y Muestra<br><br>**Población:** La población objetivo incluirá empresas que actualmente gestionan transacciones financieras en línea y aquellas que podrían beneficiarse de la implementación de la tecnología BLOCKCHAIN.<br><br>**Muestra:** Se seleccionarán empresas representativas de distintos sectores para obtener una visión más amplia de las aplicaciones de la tecnología BLOCKCHAIN.<br><br>**Métodos de Recopilación de Datos**<br>Revisión Bibliográfica: Se realizará una revisión exhaustiva de la literatura relacionada |

| | |
|---|---|
| | con la tecnología BLOCKCHAIN, sus aplicaciones y casos de estudio.<br>Estudio de Casos: Se analizarán casos de éxito en la implementación de BLOCKCHAIN en transacciones financieras y comercio electrónico.<br>Comparación de Protocolos: Se llevará a cabo un análisis detallado de los protocolos de prueba de trabajo y prueba de participación, utilizando datos cuantitativos para evaluar su eficiencia y seguridad. |
| **Conceptos adquiridos:** | **1. Tipos de BLOCKCHAIN y su Aplicabilidad en Transacciones Financieras**<br><br>Durante la investigación, se profundizó en los diversos tipos de BLOCKCHAIN existentes, evaluando su aplicabilidad específica en la validación de transacciones financieras. Se consideraron factores críticos como la velocidad de procesamiento, el grado de descentralización y la seguridad en la gestión de datos sensibles. Este análisis permitió identificar las características clave de cada tipo de BLOCKCHAIN y su idoneidad para entornos financieros.<br><br>**2. Comparación de Protocolos de Prueba de Trabajo y Prueba de Participación**<br><br>Se llevó a cabo una comparación exhaustiva entre los protocolos de prueba de trabajo y prueba de participación, explorando detalladamente su funcionamiento en la validación de bloques. Este análisis incluyó una evaluación de sus ventajas y desventajas en términos de consumo energético, seguridad y escalabilidad. La comprensión de estos protocolos proporcionó una base sólida para discernir su aplicabilidad en entornos específicos de transacciones financieras. |

| | |
|---|---|
| | **3. Casos de Éxito en Comercio Electrónico respaldado por BLOCKCHAIN**<br><br>A través de la revisión de casos de éxito en la implementación de BLOCKCHAIN en el comercio electrónico, se destacaron ejemplos específicos que ilustran cómo esta tecnología garantiza una alta confiabilidad en la gestión de transacciones financieras que involucran diferentes activos. La inmutabilidad y transparencia de la información en la BLOCKCHAIN emergieron como elementos fundamentales que contribuyen a la confianza en el comercio electrónico respaldado por esta tecnología.<br><br>**4. Utilización de Criptomonedas y Tokens como Medios de Pago Descentralizados**<br><br>Se realizó un análisis técnico detallado para justificar cómo las criptomonedas y tokens pueden ser utilizados como medios de pago descentralizados. Esto incluyó la consideración de la infraestructura de la BLOCKCHAIN a la que pertenecen, así como cómo su valor puede fluctuar en función de la demanda del mercado y el desempeño de la red en términos de eficiencia y seguridad. Este análisis proporcionó perspectivas valiosas sobre las posibles aplicaciones prácticas de las criptomonedas en transacciones seguras y descentralizadas.<br><br>A través de la consecución de estos objetivos específicos, se obtuvieron conocimientos fundamentales que contribuyen a la comprensión integral de cómo la tecnología BLOCKCHAIN puede mejorar la seguridad y confiabilidad de las transacciones financieras, ofreciendo soluciones innovadoras en el ámbito de la ciberseguridad. |

| | |
|---|---|
| **Conclusiones:** | El protocolo PoA es la mejor opción para la protección de transacciones financieras en Colombia, ya que ofrece un equilibrio óptimo entre seguridad, eficiencia y descentralización. PoA es más seguro que otros protocolos, como PoW y PoS, ya que no requiere que los nodos resuelvan algoritmos criptográficos complejos. Esto lo hace más eficiente en términos de consumo de energía y costos. Además, PoA es más descentralizado que otros protocolos, ya que no requiere que los nodos tengan que invertir en hardware especializado, además la normativa ISO 20022 versión 2019 también es un factor importante para la seguridad de las transacciones financieras en Colombia. Esta normativa proporciona directrices y mejores prácticas para la implementación de sistemas basados en BLOCKCHAIN, asegurando la interoperabilidad, la seguridad y la confidencialidad de los datos.<br><br>La adopción de la tecnología BLOCKCHAIN en el sistema financiero colombiano tendría un impacto positivo significativo en términos de eficiencia, transparencia, seguridad y confianza. En cuanto a la eficiencia, esta tecnología podría reducir los tiempos de procesamiento de pagos y eliminar intermediarios costosos, mejorando la eficiencia en las transacciones financieras y reduciendo los costos para consumidores y empresas. Además, en términos de transparencia, proporcionaría un registro mucho más confiable, ayudando a prevenir fraudes y aumentar la confianza en el sistema financiero. En cuanto a la seguridad, la BLOCKCHAIN ofrecería una mayor protección contra fraudes y garantizaría una gestión más confiable de los activos financieros, contribuyendo así a mejorar la seguridad financiera en Colombia, sin embargo, es importante destacar que la implementación efectiva de esta tecnología requiere la colaboración y participación de diferentes actores, así como la consideración de aspectos clave como la interoperabilidad entre |

| | |
|---|---|
| | sistemas existentes, la seguridad cibernética y la capacitación adecuada de los profesionales. Con estos elementos en su lugar, la adopción de la BLOCKCHAIN podría ofrecer un impulso significativo a la eficiencia y la confianza en el sistema financiero colombiano.<br><br>Las transacciones de tokens o criptoactivos en una BLOCKCHAIN representan un avance significativo en la forma en que se llevan a cabo las operaciones financieras. Esta tecnología no solo mejora la seguridad y la transparencia, sino que también ofrece la posibilidad de una mayor eficiencia, reducción de costos y accesibilidad global. A medida que continúa evolucionando, la BLOCKCHAIN tiene el potencial de cambiar fundamentalmente la forma en que interactuamos con los activos y las transacciones en la economía global. |