BLOCKCHAIN Y CRIPTOMONEDAS EN COLOMBIA: EXPLORACIÓN DE AMENAZAS EMERGENTES Y ESTRATEGIAS DE SEGURIDAD EN EL UNIVERSO DIGITAL

JESENNIA HELISABETH DUARTE MENA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C
2024

BLOCKCHAIN Y CRIPTOMONEDAS EN COLOMBIA: EXPLORACIÓN DE AMENAZAS EMERGENTES Y ESTRATEGIAS DE SEGURIDAD EN EL UNIVERSO DIGITAL

JESENNIA HELISABETH DUARTE MENA

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

EDGAR ROBERTO DULCE VILLARREAL
Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C
2024

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

DEDICATORIA

Me permito dedicar esta monografía a todas las mentes inquietas que buscan comprender y transformar el mundo digital. Con gran afecto y orgullo a mi familia, por su apoyo inquebrantable a lo largo de esta travesía académica, por su ánimo y comprensión en los momentos de dedicación extrema. A mis profesores quienes me brindaron valiosas enseñanzas que han sido invaluables.

Que este trabajo sea un humilde tributo a todos aquellos que, como yo, se sienten fascinados por el potencial de la tecnología y que este esfuerzo contribuya a una comprensión más profunda de las amenazas y desafíos en el universo digital y que sirva como guía para el fortalecimiento de la seguridad en nuestra nación con un futuro más seguro y prometedor.

AGRADECIMIENTOS

Quiero expresar mi sincero agradecimiento a las directivas de la Universidad Nacional Abierta y a Distancia UNAD y todas las personas que contribuyeron y nos brindan la oportunidad de estudiar y me acompañaron en el proceso de realización de esta monografía sobre Blockchain, por ello les reconozco que sin su apoyo y colaboración éste logro no hubiera sido posible.

También quiero mostrar mi gratitud a mi familia por su constante apoyo y aliento durante todo este proceso. Sus palabras de ánimo y comprensión fueron mi fuente de inspiración.

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE CUADROS

Pág.

GLOSARIO

AML: significa antilavado o blanqueo de capitales y se refiere a las prácticas ilegales utilizadas para ocultar el origen del dinero obtenido de manera ilícita con el fin de hacerlo parecer que proviene de fuentes legítimas.[1]

BLOCK HEIGHT: hace referencia al número de bloque actual en una blockchain, define la posición en la cadena de un bloque confirmado que forma parte de una blockchain que registra un libro de transacciones de forma secuencial en estructuras de datos conocidas como bloques.[2]

COLOMBIA FINTECH: es una asociación en Colombia que promueve y representa a las empresas y emprendedores del sector de tecnología financiera en el país. Su objetivo principal es impulsar la innovación en servicios financieros y tecnología a través de la colaboración y la creación de un ecosistema fintech sólido en Colombia.[3]

CIFRADO: es la conversión de datos de un formato legible a un formato codificado y solo se pueden leer o procesar luego de descifrarlos.[4]

EXCHANGE: es una plataforma en la que se realizan los intercambios de estas divisas digitales, es fundamental a la hora de comenzar a invertir, dado que debe

[1] AML, QUÉ es y cómo implementarlo en tu negocio | Veridas [Anónimo]. Veridas [página web]. [Consultado el 20, octubre, 2023]. Disponible en Internet: <https://veridas.com/es/que-es-aml/#:~:text=Las%20siglas%20AML%20provienen%20del,que%20proviene%20de%20fuentes%20legítimas.>.

[2] WHAT IS the block height? [Anónimo]. Bit2Me Academy [página web]. [Consultado el 20, octubre, 2023]. Disponible en Internet: <https://academy.bit2me.com/en/what-is-block-height/>.

[3] COLOMBIA FINTECH - Asociación Colombiana de Empresas de Tecnología e Innovación Financiera [Anónimo]. Colombiafintech [página web]. [Consultado el 20, octubre, 2023]. Disponible en Internet: <https://colombiafintech.co/>.

[4] ¿QUÉ ES el cifrado de datos? Definición y explicación [Anónimo]. latam.kaspersky.com [página web]. [Consultado el 20, octubre, 2023]. Disponible en Internet: <https://latam.kaspersky.com/resource-center/definitions/encryption>.

generar la confianza necesaria al usuario, que buscará operar de manera ágil y efectiva.[5]

FIREWALL: es un sistema de seguridad de red de las computadoras que restringe el tráfico de Internet entrante, saliente o dentro de una red privada, pueden considerarse fronteras o puertas que administran el flujo de la actividad web que se permite o prohíbe en una red privada.[6]

HASH: un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija.[7]

MALWARE: término que abarca cualquier tipo de software malicioso diseñado para dañar cualquier dispositivo, servicio o red programable, está conformado por todo tipo de software malicioso, incluidos los virus y los delincuentes cibernéticos lo usan por muchos motivos.[8]

PARCHE: es una pieza de software que corrige una o más vulnerabilidades de un software, que van descubriendo mediante la publicación de actualizaciones o nuevas versiones.[9]

---

[5] ¿QUÉ ES Un Exchange De Criptomonedas - Bitso Blog [Anónimo]? Bitso Blog [página web]. [Consultado el 21, octubre, 2023]. Disponible en Internet: <https://blog.bitso.com/es-co/criptomonedas-co/que-es-un-exchange-de-criptomonedas>.

[6] ¿QUÉ ES un firewall? Definición y explicación [Anónimo]. latam.kaspersky.com [página web]. [Consultado el 20, octubre, 2023]. Disponible en Internet: <https://latam.kaspersky.com/resource-center/definitions/firewall>.

[7] ¿QUÉ ES Un Hash Y Cómo Funciona? [Anónimo]. Soluciones de Ciberseguridad Kaspersky para hogar y negocio | Kaspersky | Kaspersky [página web]. [Consultado el 20, octubre, 2023]. Disponible en Internet: <https://latam.kaspersky.com/blog/que-es-un-hash-y-como-funciona/2806/>.

[8] MCAFEE. ¿Qué es el malware? | McAfee. McAfee [página web]. (15, mayo, 2020). [Consultado el 20, octubre, 2023]. Disponible en Internet: <https://www.mcafee.com/es-mx/antivirus/malware.html#:~:text=Malware%20es%20un%20término%20que,víctimas%20para%20obtener%20ganancias%20financieras.>.

[9] PARCHES DE Seguridad y Actualizaciones | BCSC [Anónimo]. Inicio | BCSC [página web]. [Consultado el 20, octubre, 2023]. Disponible en Internet: <https://www.ciberseguridad.eus/ciberpedia/buenas-practicas/parches-de-seguridad-y-actualizaciones#:~:text=Un%20parche%20de%20seguridad%20o,de%20actualizaciones%20o%20nuevas%20versiones.>.

ROUTER: dirigen los datos de red mediante paquetes que contienen varios tipos de datos, comunicaciones y transmisiones donde lee esta capa, prioriza los datos y elige la mejor ruta para cada transmisión.[10]

STABLECOIN: es una criptomoneda con un valor fijo. Se traducen al español como "moneda estable".[11]

VIRUS: son códigos informáticos creados para infectar nuestros equipos, provocar problemas en el funcionamiento de estos o robar información. Aunque se encuentran en constante evolución y cada cierto tiempo aparecen nuevos tipos.[12]

VPN: es una herramienta de ciberseguridad que cifra la conexión a Internet para ocultar su ubicación e impedir que otros intercepten su tráfico web, asegurando su privacidad y anonimato en línea mientras navega, compra o realiza operaciones bancarias en línea.[13]

VULNERABILIDAD: es una debilidad existente en un sistema que puede ser utilizada por una persona malintencionada para comprometer su seguridad. Las vulnerabilidades pueden ser de varios tipos, pueden ser de tipo hardware, software, procedimentales o humanas y pueden ser explotadas o utilizadas por intrusos o atacantes.[14]

---

[10] ¿QUÉ ES un router? - Definición y usos [Anónimo]. Cisco [página web]. [Consultado el 20, octubre, 2023]. Disponible en Internet: <https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/what-is-a-router.html>.

[11] STABLECOIN: QUÃ© es una moneda estable / Buda.com [Anónimo]. Buda.com - Compra Bitcoin y Ethereum en Chile [página web]. [Consultado el 20, octubre, 2023]. Disponible en Internet: <https://www.buda.com/guias/stablecoin#:~:text=Una%20stablecoin%20es%20una%20criptomoneda,,%20euro,%20etc.).>.

[12] VIRUS INFORMÁTICO - Tecnología | Uniandes [Anónimo]. Tecnología | Uniandes [página web]. [Consultado el 20, octubre, 2023]. Disponible en Internet: <https://tecnologia.uniandes.edu.co/virus-informatico/>.

[13] EMPEY, Charlotte y LATTO, Nica. ¿Qué es una VPN y cómo funciona? ¿Qué es una VPN y cómo funciona? [página web]. (8, abril, 2020). [Consultado el 20, octubre, 2023]. Disponible en Internet: <https://www.avast.com/es-es/c-what-is-a-vpn>.

[14] VULNERABILIDAD [Anónimo]. Banco Santander [página web]. [Consultado el 20, octubre, 2023]. Disponible en Internet: <https://www.bancosantander.es/glosario/vulnerabilidad-informatica#:~:text=En%20informática,%20una%20vulnerabilidad%20es,malintencionada%20para%20comprometer%20su%20seguridad.>.

RESUMEN

El rápido avance de la tecnología blockchain y el crecimiento exponencial de las criptomonedas han transformado la manera en que se gestionan transacciones y se almacenan registros digitales. Sin embargo, este panorama digital en constante evolución no está exento de desafíos y riesgos significativos para la seguridad cibernética. Esta monografía se centra en una profunda exploración de las amenazas emergentes que enfrentan blockchain y las criptomonedas, así como en la identificación de estrategias de seguridad que se emplean en Colombia de manera crucial para proteger activos digitales y preservar la integridad de los registros en este universo digital.

ABSTRACT

The rapid advancement of blockchain technology and the exponential growth of cryptocurrencies have transformed the way transactions are managed and digital records are stored. However, this constantly evolving digital landscape is not without significant challenges and risks for cyber security. This monograph focuses on a deep exploration of emerging threats facing blockchain and cryptocurrencies, as well as in the identification of security strategies that are used in Colombia in a crucial way to protect digital assets and preserve the integrity of records in this digital universe.

INTRODUCCIÓN

En Colombia se ha experimentado un notorio aumento en la adopción de criptomonedas y en la integración de la tecnología blockchain en diversos sectores empresariales, este fenómeno es una manifestación de la acelerada transformación digital que se está produciendo en la sociedad y la economía colombiana.

Por ello en la actualidad los términos "blockchain" y "criptomonedas" son cada vez más familiares en el discurso empresarial y tecnológico y este factor se reconoce en gran parte, a que una de las aplicaciones más notables de la tecnología blockchain es el respaldo de las criptomonedas, lo que ha dado lugar a la creación de soluciones innovadoras, como transacciones financieras más eficientes, contratos inteligentes y aplicaciones descentralizadas.

La rápida evolución de estas tecnologías, su penetración en la sociedad y su intervención en el ámbito financiero y digital destacan la necesidad de comprender en profundidad su funcionamiento y los desafíos que plantean en términos de seguridad en el universo digital.

El propósito de esta monografía es explorar en profundidad el auge de las criptomonedas y la tecnología blockchain en Colombia, identificando amenazas emergentes y examinando las estrategias de seguridad que permitan proteger los activos digitales y los datos de los ciudadanos y empresas en este nuevo entorno. A través de este análisis, se busca proporcionar una comprensión completa de los desarrollos tecnológicos, los desafíos y las oportunidades que se presentan en el contexto colombiano en constante evolución.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

En los últimos años las criptomonedas en Colombia son más recurrentes. Solamente en el año 2022, según el New Payments Index de Mastercard, el 15 % de los colombianos hicieron transacciones en monedas digitales en valores que van desde los 100 hasta los 2.000 dólares.[15] Se ha escuchado con mayor frecuencia los términos de blockchain en diversos sectores empresariales, dado que uno de los principales casos de uso de esta tecnología es el respaldo de las criptomonedas, creando integraciones como son las transacciones financieras, contratos inteligentes y aplicaciones descentralizadas,[16] este crecimiento acelerado de las criptomonedas en Colombia ha llamado la atención no solo de los usuarios y comerciantes, sino también de actores maliciosos que buscan aprovechar las vulnerabilidades de este ecosistema digital. Según el informe de la Superintendencia Financiera de Colombia, los riesgos asociados a las transacciones en criptomonedas incluyen el uso de estas tecnologías para el lavado de activos y financiación del terrorismo, lo cual subraya la urgencia de contar con marcos regulatorios claros.[17] Además, estudios recientes muestran que el país se encuentra entre las principales naciones latinoamericanas en términos de adopción de criptomonedas, pero que carece de una infraestructura robusta para mitigar las amenazas emergentes.[18]

---

[15] CRIPTOMONEDAS: ESTO es lo que podría hacer con este tipo de activos [Anónimo]. Portafolio.co [página web]. [Consultado el 22, septiembre, 2023]. Disponible en Internet: <https://www.portafolio.co/economia/finanzas/criptomonedas-como-comenzar-a-invertir-con-divisas-digitales-en-colombia-582785>.

[16] Telefónica. (2023). Aplicaciones y casos de uso de la tecnología Blockchain. Telefónica. Recuperado de https://www.telefonica.com/es

[17] Superintendencia Financiera de Colombia. (2022). Informe sobre los riesgos de las criptomonedas en Colombia.https://www.superfinanciera.gov.co/publicaciones/10090492/sala-de-prensapublicaciones-criptoactivos-10090492/

[18] Chainalysis. (2021). Adopción de criptomonedas en América Latina. Chainalysis Global Crypto Adoption. https://www.chainalysis.com/blog/2024-global-crypto-adoption-index/

Según el portal web el Portafolio informan que, en la actualidad en Colombia, existen varios comercios como restaurantes, cafeterías, gimnasios, hoteles y joyerías que han apostado por aceptar pagos por criptomonedas. Según un reciente informe de la DIAN, en Colombia existen más de 680 negocios que aceptan este tipo de comercio.[19] Por ello, se debe tener en cuenta que este tipo de tecnologías resaltan por su acelerado crecimiento e intervención en el mundo financiero y digital, transformando la forma en que se gestionan las transacciones y se almacenan los datos en línea, aumentando significativamente el valor total de los activos digitales y a la diversificación de su uso, a medida que estas innovaciones ganan relevancia, también han atraído la atención de factores maliciosos que buscan explotar las debilidades de este ecosistema en constante evolución haciendo que surjan una serie de amenazas que representan desafíos críticos para la seguridad en el universo digital.

La Cámara Colombiana de Comercio Electrónico señala que, aunque el crecimiento del comercio digital ha impulsado el uso de criptomonedas, esto también ha resultado en una mayor exposición a riesgos relacionados con la seguridad de la información.[20] Estas amenazas incluyen el robo de claves privadas, el secuestro de cuentas de criptomonedas, ataques del 51% y la explotación de vulnerabilidades en contratos inteligentes, teniendo en cuenta lo anterior se identifica que en Colombia es importante que las compañías entiendan el blockchain como una herramienta que permite mejorar la gestión de la identidad digital, pues devuelve al consumidor

[19] CUÁNTO INVIERTEN los colombianos en criptomonedas y con qué fin [Anónimo]. Portafolio.co [página web]. (21, marzo, 2023). [Consultado el 22, septiembre, 2023]. Disponible en Internet: <https://www.portafolio.co/economia/finanzas/criptomonedas-en-colombia-cuanto-invierten-en-esos-activos-los-colombianos-580173>.

[20] APROBADO PROYECTO de Ley que regula las plataformas de intercambio de criptoactivos en Colombia. [Anónimo]. Inicio | Camara de Representantes [página web]. [Consultado el 16, julio, 2024]. Disponible en Internet: <https://www.camara.gov.co/aprobado-proyecto-de-ley-que-regula-las-plataformas-de-intercambio-de-criptoactivos-en-colombia>.

la capacidad de tener control sobre sus datos personales, en el momento de acceder a cualquier tipo de servicio en línea.[21]

Estos ataques mencionados anteriormente han resultado en la pérdida significativa de activos digitales y han generado perdida en la confianza en la seguridad de las criptomonedas. Este planteamiento del problema se enfoca en la identificación y comprensión de las amenazas emergentes y la necesidad de tener más documentación referente a las estrategias de seguridad sólidas que logran salvaguardar los activos digitales y garantizar la integridad de los registros en el contexto de blockchain y criptomonedas. Por lo tanto, abordar este problema es esencial para garantizar un entorno seguro y confiable en el que las personas puedan aprovechar todo el potencial que se ofrece para crear un registro digital seguro y transparente, al tiempo que se protegen contra las amenazas emergentes que pueden surgir en este espacio en constante evolución. La investigación y la documentación de estrategias de seguridad efectivas son cruciales para mitigar estos riesgos y promover una adopción más segura y responsable de estas tecnologías.

1.2 FORMULACIÓN DEL PROBLEMA

¿Como se prepara Colombia para afrontar las amenazas emergentes en el ámbito de blockchain y criptomonedas para garantizar la confianza de las transacciones digitales y cuáles son las estrategias de seguridad más efectivas para mitigar estos riesgos y garantizar la protección de los activos digitales?

[21] ASÍ VA la Ciberseguridad y su transformación en Latinoamérica [Anónimo]. Certicámara - Entidad pionera en certificación digital en Colombia [página web]. (6, septiembre, 2019). [Consultado el 22, septiembre, 2023]. Disponible en Internet: <https://web.certicamara.com/files/comdigicert.html>.

2 JUSTIFICACIÓN

La tecnología blockchain y las criptomonedas han revolucionado la forma en que se realizan transacciones y se almacenan datos en el mundo digital, por ello la seguridad informática en la era digital actual es un tema fundamental debido a la creciente dependencia de la tecnología y la información en nuestras vidas. Según el Informe de Ciberseguridad Global en el 2023, la creciente digitalización de la sociedad ha convertido la seguridad informática en una preocupación crítica para garantizar la integridad de las transacciones y la protección de la información.[22] La tecnología digital está en el corazón de casi todos los aspectos de la sociedad, desde las transacciones financieras y la atención médica hasta la gestión de la cadena de suministro y la comunicación.

Este tema fue elegido porque la seguridad informática es una preocupación crítica en la actualidad y está ligada a áreas como blockchain y criptomonedas. Estas tecnologías, que prometen descentralización y seguridad, también enfrentan amenazas emergentes que deben abordarse para mantener su integridad y utilidad. De acuerdo con la MIT Technology Review, los ataques del 51% representan una de las amenazas más críticas para las criptomonedas, ya que comprometen la integridad del sistema al permitir que los atacantes modifiquen las transacciones.[23] El propósito de esta monografía es explorar las amenazas emergentes y las estrategias de seguridad en el contexto de blockchain para criptomonedas. La investigación busca analizar las amenazas específicas que enfrentan las criptomonedas, como los ataques de doble gasto y los ataques del 51%, e identificar cuáles son las estrategias más efectivas que se emplean en la actualidad para mitigar estos riesgos. Como destacó Nakamoto en su White Paper de 2008, la

[22] González, R. (2023). Informe de Ciberseguridad Global 2023. Instituto de Estudios sobre Ciberseguridad. [página web]. [Consultado el 10, octubre, 2024]. Disponible en Internet: <https://ogdi.org/archivos/9985>.

[23] ORCUTT, Mike. How secure is blockchain really? MIT Technology Review [página web]. (25, abril, 2018). [Consultado el 10, octubre, 2024]. Disponible en Internet: <https://www.technologyreview.com/2018/04/25/143246/how-secure-is-blockchain-really/>.

resistencia de la blockchain está diseñada para evitar estas amenazas, aunque su mitigación sigue siendo un desafío constante.[24]

Además, se desea destacar la importancia de la educación y la concientización sobre la seguridad informática en este espacio en constante evolución. De acuerdo con un estudio de la Universidad de Cambridge, la falta de concientización sobre las amenazas digitales es uno de los mayores desafíos para la adopción segura de tecnologías descentralizadas como blockchain.[25] La relevancia de este tema radica en su aplicación práctica y en su contribución al conocimiento en el campo de la seguridad informática. A medida que las criptomonedas y la tecnología blockchain continúan expandiéndose y siendo adoptadas en diversas industrias, es esencial comprender y abordar las amenazas que enfrentan.

Esta investigación busca proporcionar información valiosa para comprender como se pueden proteger los activos digitales y fomentar un entorno seguro en el universo digital. Además, al aumentar la concientización sobre estas amenazas emergentes y las estrategias de seguridad efectivas, se espera contribuir al fortalecimiento de la comunidad digital y al uso responsable de estas tecnologías transformadoras. Como señaló McKinsey en 2021, la tecnología blockchain se está adoptando de forma creciente en sectores como la cadena de suministro, las finanzas y la salud, donde su promesa de seguridad y descentralización está generando impacto.[26]

[24] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Bitcoin.org. [Consultado el 10, octubre, 2024]. Disponible en Internet: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://bitcoin.org/bitcoin.pdf

[25] Zhang, B., & Auer, R. (2022). The global adoption of blockchain and digital currencies. University of Cambridge. [Consultado el 10, octubre, 2024]. Disponible en Internet: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2017-09-27-ccaf-globalbchain.pdf

[26] CARSON, Brant, et al. Blockchain beyond the hype: What is the strategic business value? McKinsey & Company [página web]. (19, junio, 2018). [Consultado el 10, octubre, 2024]. Disponible en Internet: <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value>.

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Analizar las características de las estrategias de seguridad utilizadas en el sector financiero de las entidades bancarias en la ciudad de Bogotá, Colombia para el entorno de blockchain y criptomonedas según la efectividad en la mitigación de amenazas emergentes más populares en la actualidad, con el fin de proporcionar una guía a los usuarios a seleccionar las estrategias más adecuadas para proteger sus activos digitales.

3.2 OBJETIVOS ESPECÍFICOS

- Caracterizar las diferencias que se presentan entre amenazas emergentes específicas que afectan a las criptomonedas y blockchain, en comparación con las amenazas más tradicionales en el ámbito de la seguridad digital, con el fin de comprender las características únicas de las amenazas emergentes.

- Identificar las percepciones y niveles de conocimiento de las personas sobre criptomonedas, identificando mitos comunes y evaluando el grado de comprensión que tienen sobre los servicios ofrecidos por esta tecnología.

- Categorizar las estrategias más populares de seguridad que se emplean en el entorno de blockchain y criptomonedas según su efectividad en la mitigación de amenazas emergentes, para identificar los beneficios que estas ofrecen en el mundo digital.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

4.1.1. Distributed Ledger Technology

Tecnología de Registros Distribuidos es un término amplio que corresponde al acrónimo DLT y se utiliza para describir una categoría de tecnologías que permiten mantener registros compartidos y sincronizados a través de múltiples nodos o participantes. La entidad IEBS con el señor Javier Hurtado público en el 2021 un artículo en el cual se comprende que este esquema de red es descentralizado, lo cual se caracteriza por permitir diseñar una estructura de sistemas que funcionen como una base de datos NO centralizada.[27] Esto significa que no existe un ordenador o servidor central que almacene la información convirtiéndolo en un sistema más seguro, por ello destaca que las probabilidades de hackear la base de datos sean bajas al no poder atacar un ordenador central.

Estudios del Foro Económico Mundial señalaron que, aunque DLT aún enfrenta desafíos, su potencial para mejorar la eficiencia de los mercados financieros, reduciendo los riesgos y los costos asociados con sistemas tradicionales de liquidación, sigue siendo prometedor.[28] Además, empresas como Amazon Web Services y Ava Labs están acelerando la adopción de blockchain en entornos empresariales, facilitando la integración de DLT en sectores como el comercio y los servicios financieros.[29] Brindando a las organizaciones una plataforma confiable para desarrollar soluciones blockchain personalizadas que puedan manejar grandes

[27] QUE SON las DLT y en que se diferencian de Blockchain [Anónimo]. Thinking for Innovation [página web]. [Consultado el 24, septiembre, 2023]. Disponible en Internet: <https://www.iebschool.com/blog/que-son-las-dlt-y-en-que-se-diferencian-de-blockchain-digital-business/>.

[28] World Economic Forum. (2023). Why distributed ledger technology needs to scale back its ambition. https://www.weforum.org/

[29] Next Move Strategy Consulting. (2023). Distributed Ledger Market Analysis 2024-2030. Disponible en: https://www.nextmsc.com/

volúmenes de datos de manera segura y eficiente. Esto permite que sectores como el financiero y el comercial no solo optimicen sus transacciones, sino que también adopten un enfoque más transparente y descentralizado.

De manera clara la empresa KPMG la cual es una red global de firmas que presta servicios de Auditoría, Impuestos y Consultoría,[30] destaca que, para instituciones financieras, el verdadero valor de la DLT radica en su capacidad de eliminar ineficiencias en los sistemas de liquidación tradicionales, especialmente a través de infraestructuras permisadas que permiten una mayor seguridad y control.[31]

4.1.2. Blockchain

En la actualidad existen diversas empresas que basan su funcionamiento en la manipulación de datos principalmente en comercios e intercambios financieros en línea; y para ello, en cuanto más rápido y precisa sea la interacción de la información mejor; la tecnología de Blockchain se ha convertido en una herramienta ideal para ofrecer esa información porque proporciona una interacción inmediata, compartida y completamente transparente almacenada en un libro mayor inmodificable al que solo pueden acceder los miembros de la red con permisos.[32]

El blockchain es una tecnología de registro distribuido que se utiliza para mantener un registro seguro y público de transacciones y se encuentran bajo el paraguas del DLT. Es un sistema digital que permite a los usuarios y sistemas registrar transacciones relacionadas con activos, funcionando como una cadena de bloques, donde cada bloque contiene una serie de transacciones y está vinculado al bloque anterior, de esta forma inmutable manteniendo el registro distribuido almacenando

[30] ¿Quiénes Somos? (s.f.). KPMG. https://kpmg.com/co/es/home/about/quienes-somos.html
[31] KPMG International | Home. (s.f.). KPMG. https://kpmg.com/xx/en.html
[32] ¿QUÉ ES la tecnología blockchain? - IBM Blockchain | IBM [Anónimo]. Mit watsonx die Leistung der KI multiplizieren | IBM [página web]. [Consultado el 24, septiembre, 2023]. Disponible en Internet: <https://www.ibm.com/es-es/topics/blockchain>.

la información en múltiples ubicaciones en un momento dado.[33] Al ser una tecnología innovadora que proporciona una forma segura y transparente de registrar y verificar transacciones, su potencial de aplicación se extiende más allá de las criptomonedas.

4.1.7. Activos digitales

Los activos digitales son representaciones electrónicas de valor que existen exclusivamente en formato digital de acuerdo con el artículo del señor Luis Velásquez de la consultora Inusual, argumentó que son elementos intangibles que forman parte del patrimonio de una organización y generan un valor monetario,[34] esta definición se complementa con el artículo de la empresa Punto Desing Xperience que define el conjunto de capacidades, funcionalidades o elementos en general que están en servicios en línea y que están dispuestos para que los usuarios realicen algunas tareas, como la compra, la solución de problemas, el aprendizaje, entre otras.[35] Estos incluyen criptomonedas, tokens, acciones digitales y otros activos financieros que se almacenan y transfieren en línea.

---

[33] ACUÑA, Wilder Pereyra. ¿Qué es Blockchain o Tecnología de Registro Distribuido (DLT)? Blog - Escuela Posgrado - Universidad Continental [página web]. (10, mayo, 2022). [Consultado el 24, septiembre, 2023]. Disponible en Internet: <https://blogposgrado.ucontinental.edu.pe/blockchain-tecnologia-registro-distribuido-dlt#:~:text=El%20blockchain%20es%20una%20de,ubicaciones%20en%20un%20momento%20dado.>.

[34] ¿QUÉ SON los activos digitales y por qué son importantes en tu empresa? [Anónimo]. Consultora Inusual [página web]. [Consultado el 24, septiembre, 2023]. Disponible en Internet: <https://cinusual.com/que-son-los-activos-digitales-y-por-que-son-importantes-en-tu-empresa>.

[35] ¿QUÉ SON los activos digitales? Ejemplos y cómo administrarlos [Anónimo]. Xperience Design - Agencia de diseño de servicios [página web]. [Consultado el 25, septiembre, 2023]. Disponible en Internet: <https://www.xperiencedesign.co/blog/qué-son-los-activos-digitales-dos-perspectivas-para-unconcepto#:~:text=Desde%20una%20primera%20perspectiva,%20los,los%20datos%20recolectados, %20entre%20otros.>.

4.1.3. Criptomonedas

El Banco Santander S.A realizo una publicación en el 2022 donde consideran un activo digital a las criptomonedas y se emplea un cifrado criptográfico para garantizar su titularidad y asegurar la integridad de las transacciones y controlar la creación de unidades adicionales, es decir, evitar que alguien pueda hacer copias,[36] por ejemplo, con una foto. Las criptomonedas son monedas digitales o virtuales que utilizan criptografía para asegurar las transacciones, por lo cual existen exclusivamente en formato digital y no tienen una forma física como las monedas o billetes tradicionales.

Cada transacción se registra en un libro mayor digital llamado blockchain, que es inmutable y resistente a la manipulación debido a la criptografía. La empresa Kaspersky define este concepto estableciéndolo como un sistema de pago digital que no depende de bancos para verificar transacciones que al operar en un libro mayor público llamado cadena de bloques, crea un registro de todas las transacciones que actualizan los propietarios de monedas, el cual implica utilizar potencia informática para resolver problemas matemáticos complicados que generan monedas. Los usuarios también pueden comprar las divisas desde agentes, para luego almacenarlas y gastarlas mediante monederos criptográficos.[37] Es importante destacar que las criptomonedas están sujetas a volatilidad en su valor y regulaciones que pueden variar de un país a otro. Antes de involucrarse en el uso o inversión en criptomonedas, es importante comprender los riesgos y considerar cuidadosamente su idoneidad para las necesidades financieras.

[36] SANTANDER. ¿Qué son las criptomonedas y cómo funcionan? Santander Corporate Website [página web]. (12, agosto, 2021). [Consultado el 24, septiembre, 2023]. Disponible en Internet: <https://www.santander.com/es/stories/guia-para-saber-que-son-las-criptomonedas>.

[37] ¿QUÉ ES una criptomoneda y cómo funciona? [Anónimo]. latam.kaspersky.com [página web]. [Consultado el 24, septiembre, 2023]. Disponible en Internet: <https://latam.kaspersky.com/resource-center/definitions/what-is-cryptocurrency>.

4.1.4. Criptografía

Es el desarrollo de un conjunto de técnicas que permiten alterar y modificar mensajes o archivos con el objetivo de que no puedan ser leídos por todos aquellos usuarios que no estén autorizados a hacerlo.[38] El uso de técnicas matemáticas para asegurar la privacidad y la seguridad de las transacciones en una cadena de bloques es esencial en Colombia, como en cualquier otro lugar, para proteger la información, salvaguardar la privacidad y garantizar la seguridad de las transacciones y comunicaciones en un mundo digital en constante evolución. Su relevancia se observa en numerosos aspectos de la vida cotidiana, la economía y la seguridad.

4.1.5. Bitcoin

Es una criptomoneda o moneda virtual, concretamente la primera que fue desarrollada por un anónimo conocido como Satoshi Nakamoto. Es la criptomoneda que le ha marcado el camino a todas las demás que llegaron después utilizando su tecnología. Esta tecnología es la cadena de bloques o blockchain, que también se utiliza para otras cosas.[39] Es una forma de dinero digital descentralizada que permite a las personas enviar y recibir fondos en línea de manera segura sin necesidad de intermediarios como bancos. Lo que hace que Bitcoin sea especialmente importante es su innovador sistema de contabilidad llamado blockchain, que es público y transparente. Además, Bitcoin se considera una reserva de valor digital, similar al oro y su adopción ha llevado a debates sobre el futuro del dinero y las finanzas, así

[38] ¿QUÉ ES el cifrado de datos? Definición y explicación [Anónimo]. latam.kaspersky.com [página web]. [Consultado el 11, octubre, 2023]. Disponible en Internet: <https://latam.kaspersky.com/resource-center/definitions/encryption>.

[39] FERNÁNDEZ, Yúbal. Bitcoin, guía a fondo: qué es, cómo funciona y cómo conseguirlos. Xataka - Tecnología y gadgets, móviles, informática, electrónica [página web]. (9, junio, 2023). [Consultado el 20, octubre, 2023]. Disponible en Internet: <https://www.xataka.com/basics/bitcoin-guia-a-fondo-que-como-funciona-como-conseguirlos>.

como a la exploración de nuevas formas de inversión y tecnología financiera.[40] Su importancia radica en su potencial para cambiar la forma en que se maneja el dinero y cómo se percibe la propiedad y la transferencia de activos en la era digital.

4.1.6. Universo digital

En el trascurso del 2020 al 2022 la empresa Market Team S.A realizó un estudio que indicó que las marcas han comenzado a trabajar en colaboración con artistas digitales para la creación de NTFs del universo digital,[41] para la conexión monetaria entre el mundo real y virtual haciendo referencia a un mundo virtual ficticio o un espacio virtual colectivo y compartido con frecuencia creado por convergencia y compatibilización con un aspecto de la realidad externa.[42] En esencia, se trata de una realidad virtual a gran escala que va más allá de los mundos virtuales y juegos en línea tradicionales y se ha popularizado recientemente y está siendo explorado y desarrollado por empresas de tecnología y entretenimiento, así como por investigadores. Aunque todavía está en sus primeras etapas, el concepto del metaverso representa una visión futurista de un espacio digital compartido y altamente interactivo que podría transformar la forma en que se trabaja, se juega, se aprende y se interactúa en línea.

---

[40] ¿CUÁL ES la importancia del Bitcoin? - News America Digital [Anónimo]. News America Digital [página web]. [Consultado el 20, octubre, 2023]. Disponible en Internet: <https://news.america-digital.com/que-es-bitcoin/>.

[41] COLABORADORES DE LOS PROYECTOS WIKIMEDIA. Metaverso - Wikipedia, la enciclopedia libre. Wikipedia, la enciclopedia libre [página web]. (25, mayo, 2007). [Consultado el 24, septiembre, 2023]. Disponible en Internet: <https://es.wikipedia.org/wiki/Metaverso#:~:text=%20En%20la%20novela%20el, aspecto%20de%20la%20realidad%20externa.>.

[42] LAS NFTS, universos digitales (metaverso) y por qué las grandes marcas las están involucrando en sus estrategias de marketing y comercialización. [Anónimo]. Market Team S.A [página web]. [Consultado el 24, septiembre, 2023]. Disponible en Internet: <https://www.linkedin.com/pulse/las-nfts-universos-digitales-metaverso-y-por-qué-grandes-/?originalSubdomain=es>.

4.1.8. Contratos inteligentes

La universidad del externado de Colombia informa que el termino de contratos inteligentes puede ser entendido como un código escrito en lenguaje de programación que corre en una plataforma segura como Blockchain, lo que hace inmodificable y autoejecutable, excluyendo el elemento humano en la ejecución del contrato y su autonomía se deriva del hecho de que las redes Blockchain operan sin ninguna entidad central o confiable que equipare.[43]

Este tipo de software se caracteriza por llevar a cabo una serie de actividades previamente introducidas este factor le permite seguir creciendo en la industria. Por ello, se espera que desempeñen un papel cada vez más relevante en la economía digital y en la transformación de los modelos comerciales tradicionales. La señora Isabel Pérez en su artículo de Criptonoticias, anuncia que el cumplimiento de este tipo de contratos no está sujeto a la interpretación de ninguna de las partes: si el evento A sucede, entonces la consecuencia B se pondrá en marcha de forma automática. No se requiere de ningún intermediario, pues este papel lo adopta el código informático, que asegurará sin dudas el cumplimiento de las condiciones.[44]

[43] ¿QUÉ ES un contrato inteligente? - Departamento de Propiedad Intelectual [Anónimo]. Departamento de Propiedad Intelectual [página web]. [Consultado el 25, septiembre, 2023]. Disponible en Internet: <https://propintel.uexternado.edu.co/que-es-un-contrato-inteligente/>.
[44] QUÉ SON los contratos inteligentes [Anónimo]. CriptoNoticias - Noticias de Bitcoin, Ethereum y criptomonedas [página web]. [Consultado el 24, septiembre, 2023]. Disponible en Internet: <https://www.criptonoticias.com/criptopedia-old/que-son-contratos-inteligentes-blockchain-criptomonedas/>.

4.1.9. Seguridad informática

Es un campo de la tecnología de la información que se enfoca en proteger los sistemas de datos, por lo que la universidad de Cataluña resalta que esta temática se basa en un conjunto de prácticas, estrategias, métodos, herramientas y procedimientos cuyo objetivo final es garantizar la integridad de los equipos informáticos y de la información que contienen. Su principal objetivo es que, tanto personas como equipos tecnológicos y datos, estén protegidos contra daños y amenazas hechas por terceros.[45] Desempeñando un papel esencial en áreas tecnológicas como son las criptomonedas, principalmente para proteger los activos digitales, transacciones y la confianza de los usuarios. Las medidas de seguridad adecuadas, como el uso de billeteras seguras, autenticación de dos factores, son prácticas esenciales para garantizar una experiencia segura en el mundo de las criptomonedas.

4.1.10. Ciberseguridad

Es la práctica de proteger equipos, redes, aplicaciones de software, sistemas críticos y datos de posibles amenazas digitales. Las organizaciones tienen la responsabilidad de proteger los datos para mantener la confianza del cliente y cumplir la normativa.[46] En un mundo en constante evolución tecnológica, la ciberseguridad se ha convertido en una necesidad, para salvaguardar nuestras

[45] SEGURIDAD INFORMÁTICA: La importancia y lo que debe saber [Anónimo]. Educación Sin Fronteras | UdeCataluña [página web]. [Consultado el 24, septiembre, 2023]. Disponible en Internet: <https://www.ucatalunya.edu.co/blog/seguridad-informatica-la-importancia-y-lo-que-debe-saber>.

[46] ¿QUÉ ES la ciberseguridad? - Explicación de la ciberseguridad - AWS [Anónimo]. Amazon Web Services, Inc. [página web]. [Consultado el 1, octubre, 2023]. Disponible en Internet: <https://aws.amazon.com/es/what-is/cybersecurity/#:~:text=La%20ciberseguridad%20es%20la%20práctica,cliente%20y%20cumplir%20la%20normativa.>.

vidas digitales, sino también para garantizar la estabilidad y la seguridad de la sociedad y la economía en su conjunto.

Desempeña un papel vital en la protección de la seguridad nacional, desde la infraestructura crítica hasta los sistemas de defensa y la información gubernamental, la seguridad en línea es fundamental para prevenir ataques cibernéticos que podrían poner en peligro la seguridad del país. Las empresas dependen de la tecnología y la información digital para operar eficazmente y un ataque cibernético puede tener impactos devastadores en términos de pérdida de datos, costos financieros y daño a la reputación.

4.1.11. Amenazas emergentes

Los riesgos emergentes, por definición, presentan baja probabilidad de ocurrencia y alto impacto negativo. Así es que estas son dos características iniciales que permiten identificarlos por ello son catalogados como un riesgo o desafío que está surgiendo o evolucionando en un determinado contexto, como la tecnología, la seguridad, la sociedad o el medio ambiente.[47] Estas amenazas suelen ser nuevas o haber adquirido recientemente una mayor relevancia debido a cambios en el entorno. Las amenazas emergentes pueden tomar muchas formas y pueden ser impredecibles en su impacto y alcance.

[47] GESTIÓN DE riesgos emergentes: cómo identificar amenazas de baja probabilidad y alto impacto a tiempo [Anónimo]. Escuela Europea de Excelencia [página web]. [Consultado el 24, septiembre, 2023]. Disponible en Internet: <https://www.escuelaeuropeaexcelencia.com/2022/03/gestion-de-riesgos-emergentes-como-identificar-amenazas-de-baja-probabilidad-y-alto-impacto-a-tiempo/>.

4.1.12. Ciberataque

En la actualidad las empresas cuentan con múltiples sistemas de información y bases de datos ya sea en infraestructuras físicas como en la nube, por lo tanto varia la representación de las amenazas para la protección de la información, teniendo en cuenta esta información la empresa Microsoft informa que los ciberataques vienen en diferentes formas a través de sistemas y redes de equipos por lo que se reconocen como el conjunto de acciones dirigidas contra sistemas de información, como pueden ser bases de datos o redes computacionales, con el objetivo de perjudicar a personas, instituciones o empresas. Este tipo de acción puede atentar tanto contra los equipos y sistemas que operan en la red, anulando sus servicios, como contra bases que almacenan información, la cual puede ser espiada, robada o incluso, utilizada para extorsionar.[48] Estos ataques pueden variar en complejidad y motivación, pero todos representan una amenaza seria para la seguridad cibernética.

4.1.13. Tokenización de Activos

La tokenización de activos está emergiendo como una solución innovadora en la industria financiera, permitiendo transformar activos físicos y financieros en representaciones digitales dentro de una red blockchain. Este proceso permite fraccionar la propiedad de activos previamente ilíquidos, como inmuebles o arte, en múltiples tokens que pueden ser comprados y comercializados de manera más accesible y eficiente. Esto otorga a los inversores una mayor participación en mercados anteriormente reservados para grandes fortunas, mejorando la liquidez y facilitando la diversificación de carteras a menor costo.[49]

---

[48] IBERDROLA. Ciberataques. Iberdrola [página web]. (30, junio, 2021). [Consultado el 25, septiembre, 2023]. Disponible en Internet: <https://www.iberdrola.com/innovacion/ciberataques>.
[49] Suiza, B. (2024, 5 de abril). Lección 6: Tokenización de activos | BBVA CH. BBVA Suiza - Banca privada online| BBVA Suiza. https://www.bbva.ch/blog/educacion-financiera/blockchain-to-

Adicionalmente, la tokenización elimina la necesidad de intermediarios tradicionales en las transacciones, lo que incrementa la automatización y reduce los costos asociados a la gestión de activos. Gracias a la Distributed Ledger Technology (DLT), las transacciones son inmutables y programadas mediante contratos inteligentes que aseguran la transparencia y eficiencia en la gestión de los tokens. A medida que la tokenización gana popularidad, se estima que tendrá un impacto significativo en los mercados financieros, con una proyección de 16 billones de dólares en activos tokenizados para 2030, lo que indica su enorme potencial de crecimiento en las próximas décadas.[50]

4.1.14. Ataques de doble gasto

Este tipo de comercio y transacciones económicas en el mundo digital presenta muchas variables y factores de riesgos dado que en la actualidad los ciber delincuentes mejoran sus técnicas de robo, la academia bit2m informa que el modo de operar de esta técnica consiste cuando un usuario desea utilizar las mismas monedas múltiples veces y para lograrlo, realiza dos transacciones al mismo tiempo para comprar los productos a los vendedores. En ese momento, comienzan a generar los bloqueos y a validar las transacciones. Pero en un punto, uno de los bloques se transmitirá a más nodos de manera más rápida, mientras que el otro no. Por lo que solo un bloque será confirmado.[51] Esto plantea riesgos significativos en sistemas descentralizados y es crucial para la seguridad de las criptomonedas y la integridad de los sistemas de Blockchain.

---

go/leccion-6-tokenizacion-de-activos-la-maquina-cripto-empieza-a-funcionar.html#:~:text=Tokenizar%20significa%20transformar%20y%20representar,o%20emitir%20bonos%20y%20participaciones.

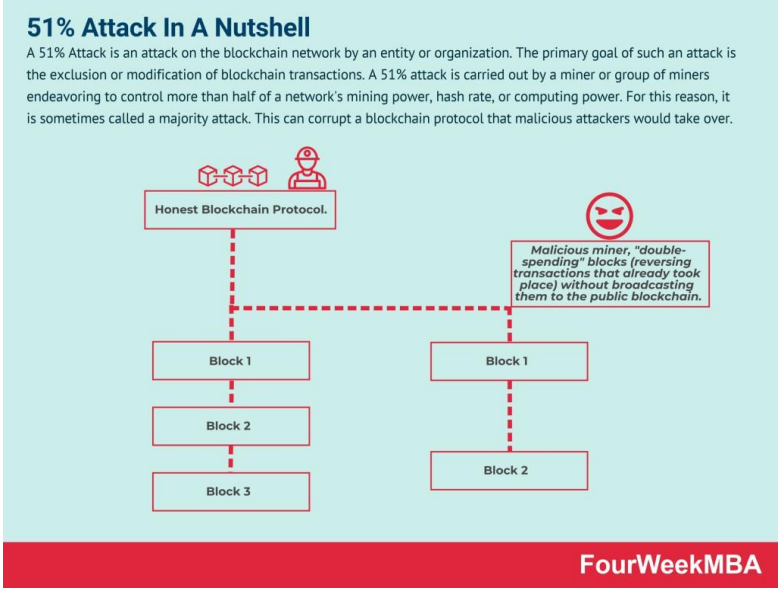
[50] Noya, E. (2023). El sector financiero y la tokenización de activos. https://cincodias.elpais.com/cincodias/2023/12/27/idearium/1703674899_140632.html

[51] ¿QUÉ ES el doble gasto? [Anónimo]. Bit2Me Academy [página web]. [Consultado el 26, septiembre, 2023]. Disponible en Internet: <https://academy.bit2me.com/que-es-doble-gasto/>.

4.1.15. Ataques del 51%

El señor Genaro Cuofano de la empresa FourWeekMBA el 29 de junio del 2023 realizó una publicación en la cual analiza que un ataque del 51% puede ser ejecutado por un minero o grupo de mineros que intentan controlar más de la mitad del sistema, el poder de minería, la tasa de hash o el poder de cómputo que puede corromper un protocolo de cadena de bloques que los atacantes maliciosos tomarían.[52] Esto les otorga un poder desproporcionado para manipular transacciones, lo que podría permitirles realizar gastos dobles o tomar el control de la red, comprometiendo su seguridad y confiabilidad. Este tipo de ataque es una preocupación importante en sistemas blockchain descentralizados.

Figura 1. Esquema de ataque del 51%



Fuente: Cuofano (2023). Modelos comerciales que se aplican en la secuencia de ataque. Imagen tomada de: https://fourweekmba.com/es/Ataque-51/

[52] ATAQUE DEL 51 % y por qué es importante comprender los modelos de negocio de Blockchain - FourWeekMBA [Anónimo]. FourWeekMBA [página web]. (29, junio, 2023). [Consultado el 25, septiembre, 2023]. Disponible en Internet: <https://fourweekmba.com/es/Ataque-51/>.

4.1.16. Criptoeconomía

Es un campo que combina la economía, la criptografía y la informática para estudiar el diseño y la implementación de protocolos seguros y eficientes para sistemas descentralizados,[53] donde se aplican principios económicos, incluyendo la emisión y distribución de tokens.

4.1.17. Finanzas Descentralizadas

Las finanzas descentralizadas (DeFi), impulsadas principalmente por plataformas como Ethereum, han transformado la forma en que se gestionan y se utilizan los activos financieros digitales. Las DeFi permiten realizar transacciones financieras sin intermediarios, utilizando contratos inteligentes para ofrecer servicios como préstamos, intercambio de activos y depósitos.[54] Esta descentralización elimina la necesidad de bancos u otras entidades tradicionales, lo que reduce costos y democratiza el acceso a estos servicios, especialmente en regiones con infraestructuras financieras limitadas.

Además, el crecimiento del uso de las finanzas descentralizadas ha sido exponencial a nivel global, con un notable aumento en la cantidad de usuarios e inversores que prefieren esta nueva tecnología para manejar sus activos digitales.[55]

---

[53] ¿QUÉ ES criptografía? [Anónimo]. NIC Argentina [página web]. [Consultado el 19, octubre, 2023]. Disponible en Internet: <https://nic.ar/es/enterate/novedades/que-es-criptografia#:~:text=La%20criptografía%20es%20el%20desarrollo,no%20estén%20autorizados%20a%20hacerlo.>.

[54] Finanzas descentralizadas (DeFi) en Ethereum: Todo lo que necesitas saber sobre la Finanzas descentralizadas (DeFi) en Ethereum. (2024). Nuevatribuna. https://www.nuevatribuna.es/articulo/sociedad/todo-necesitas-saber-finanzas-descentralizadas-defi-ethereum/20240924174749230850.html

[55] Aumenta el uso de las finanzas descentralizadas a nivel global - Dirigentes Digital. (2024). Dirigentes. https://dirigentesdigital.com/funds-markets/cripto/aumenta-el-uso-de-las-finanzas-descentralizadas-a-nivel-global/

Esta tendencia refleja no solo la creciente confianza en los sistemas descentralizados, sino también una respuesta a la demanda de mayor transparencia y seguridad en las transacciones financieras, siendo un factor clave en el desarrollo futuro de la economía digital global.

4.2 MARCO CONCEPTUAL

4.2.1. Diferencias entre Blockchain y las Bases de datos distribuidas.

Blockchain y las bases de datos distribuidas son dos tecnologías relacionadas que tienen algunas similitudes, pero también diferencias significativas en términos de estructura, funcionamiento y casos de uso, cuando las personas se refieren a Blockchain, normalmente hacen referencia a un sistema distribuido sin control centralizado, mientras que las bases de datos distribuidas son sistemas distribuidos que tienen una autoridad central. Por esta razón, la principal característica diferencial de la tecnología DLT/Blockchain es la garantía de la integridad de los datos que son almacenados.[56] Son tecnologías distintas entre ellas y depende de los requisitos específicos de la aplicación y de los compromisos en términos de seguridad, escalabilidad y eficiencia, como se evidencia en el siguiente cuadro comparativo:

Cuadro 1. Aspectos Comparativos.

Aspecto	Blockchain	Bases de Datos Distribuidas
Estructura de Datos	Cadena de bloques	Variedad de estructuras
Consenso	Prueba de trabajo (PoW), Prueba de Participación (PoS)	Diversos mecanismos de consenso
Seguridad	Alta seguridad debido a la inmutabilidad y resistencia a la censura	Seguridad depende de la configuración y el control de acceso
Escalabilidad	Menos escalable debido a los mecanismos de consenso y duplicación de datos	Puede ser más escalable según la implementación y la tecnología

[56] DLT/BLOCKCHAIN [Anónimo]. mintic.gov.co [página web]. [Consultado el 25, septiembre, 2023]. Disponible en Internet: <https://mintic.gov.co/portal/715/articles-149959_recurso_1.pdf>.

Casos de Uso	Criptomonedas, contratos inteligentes, seguimiento de la cadena de suministro	Aplicaciones empresariales, aplicaciones web y móviles, sistemas de bases de datos tradicionales
Velocidad	Menos rápida debido a procesos de consenso más lentos	Potencialmente más rápida debido a la variedad de mecanismos de consenso
Flexibilidad	Menos flexible debido a la estructura rígida de cadena de bloques	Más flexible en términos de estructura de datos y organización

Fuente: Elaboración propia con base en información de páginas web de internet: [57], [58],[59].

4.2.2. Escalabilidad De Blockchain

Uno de los principales desafíos es la capacidad de la cadena de bloques para manejar un alto volumen de transacciones en un corto período de tiempo. La escalabilidad es crucial para que las blockchains se conviertan en una infraestructura confiable para aplicaciones a gran escala, como sistemas de pago globales, registros médicos electrónicos o seguimiento de la cadena de suministro. Si una cadena de bloques no puede manejar un gran número de transacciones de manera eficiente, enfrentará cuellos de botella, retrasos y costos operativos elevados.

Cuando se habla de escalabilidad en blockchains, se hace referencia incrementar su capacidad de gestionar transacciones, en donde protocolos como Bitcoin

[57] 101 Blockchains. (s.f.). Blockchain vs Base de Datos: Principales Diferencias. 101 Blockchains. Recuperado de https://101blockchains.com/es/blockchain-vs-base-de-datos/

[58] Criptonoticias. (2023). ¿Blockchain y bases de datos descentralizadas son la misma cosa? Criptonoticias. Recuperado de https://www.criptonoticias.com/tecnologia/blockchain-y-bases-de-datos-descentralizadas-son-la-misma-cosa/

[59] Gómez, F. (2017). Blockchain: La nueva base de datos No SQL en Big Data. Universidad Libre. Recuperado de https://repository.unilibre.edu.co/bitstream/handle/10901/11220/BLOCKCHAIN%20LA%20NUEVA%20BASE%20DE%20DATOS%20NO%20SQL%20EN%20BIG%20DATA.pdf?sequence=1&isAllowed=y

presentan múltiples fortalezas, pero la escalabilidad no es una de ellas. Si Bitcoin se ejecutara en una base de datos controlada de manera centralizada, resultaría relativamente fácil para el administrador incrementar la velocidad y tasa de transferencia.[60] A medida que se trabaja en superar estos desafíos, es probable que se observe un mayor uso de las blockchains en una variedad de aplicaciones y una mayor integración en la vida cotidiana.

4.2.3. Seguridad En Blockchain

Es uno de los pilares fundamentales que hacen que esta tecnología sea tan atractiva y confiable en un mundo cada vez más digital. La seguridad en una blockchain se basa en una combinación de características técnicas que la hacen resistente a la manipulación y la corrupción de datos, se basa en la descentralización, la criptografía, la inmutabilidad y la transparencia. Es un sistema integral de gestión de riesgos para una red de blockchain, que utiliza estructuras de ciberseguridad, servicios de garantía y mejores prácticas para reducir los riesgos contra ataques y fraudes.[61]

- **Descentralización**: es el concepto de dividir las funciones de un sistema entre numerosas unidades independientes, las blockchains operan en una red descentralizada de nodos, lo que hace que sea increíblemente difícil alterar la información.[62] Para manipular la red, un atacante tendría que

[60] Binance Academy [página web]. (20, febrero, 2020). [Consultado el 2, octubre, 2023]. Disponible en Internet: <https://academy.binance.com/es/articles/blockchain-scalability-sidechains-and-payment-channels>.
[61] ¿QUÉ ES la seguridad de blockchain? | IBM [Anónimo]. IBM in Deutschland, Österreich und der Schweiz | IBM [página web]. [Consultado el 20, septiembre, 2023]. Disponible en Internet: <https://www.ibm.com/es-es/topics/blockchain-security#:~:text=IBM-,¿Qué%20es%20la%20seguridad%20de%20blockchain?,riesgos%20contra%20ataques%20y%20fraudes.>.
[62] BLOCKCHAIN: QUÉ es la descentralización y qué hay que saber para aprovechar las posibilidades que ofrece [Anónimo]. A24 [página web]. (3, marzo, 2023). [Consultado el 12, septiembre, 2023].

controlar la mayoría de los nodos, lo que resulta altamente improbable en blockchains maduras y bien establecidas.

- **Criptografía**: Las transacciones y los datos en una blockchain están protegidos mediante técnicas de criptografía avanzada. La información se almacena de manera segura en bloques que están interconectados y sellados por complejos algoritmos criptográficos. Esto hace que sea extremadamente difícil modificar datos sin ser detectado.

- **Consensos Robustos:** La mayoría de las blockchains utilizan algoritmos de consenso, como la Prueba de Trabajo (PoW) o la Prueba de Participación (PoS), para validar transacciones y acordar el estado de la cadena. Estos sistemas requieren que los nodos lleguen a un consenso antes de que se agregue nueva información, lo que previene ataques maliciosos.

- **Inmutabilidad:** tiene el potencial de transformar el proceso de auditoría en un procedimiento rápido, eficiente y rentable, brindando más confianza e integridad a los datos que las empresas usan y comparten todos los días.[63] Una vez que los datos se registran en un bloque y se confirman mediante el consenso, resulta extremadamente difícil alterarlos o eliminarlos. Esto convierte que las blockchains sean ideales para mantener registros inmutables, como contratos inteligentes o registros de propiedad.

- **Transparencia:** contribuye a construir la confianza y la seguridad entre los donantes, ya que pueden verificar que sus fondos se utilizan para el propósito

Disponible en Internet: <https://www.a24.com/crypto/blockchain-que-es-la-descentralizacion-y-que-hay-que-saber-aprovechar-las-posibilidades-que-ofrece-n1081251>.

[63] MORALES, Carlos Rodríguez. Blockchain y ciberseguridad: la inmutabilidad (II). Telefónica Tech [página web]. (19, septiembre, 2019). [Consultado el 14, septiembre, 2023]. Disponible en Internet: <https://telefonicatech.com/blog/blockchain-y-ciberseguridad-la-inmutabilidad#:~:text=La%20inmutabilidad,%20la%20capacidad%20para,destaca%20como%20un%20beneficio%20clave.>.

previsto.[64] Las transacciones en una blockchain son transparentes y verificables por cualquiera. Esto fomenta la confianza y la responsabilidad en el sistema, ya que cualquiera puede auditar la cadena y verificar su integridad.

Estas características hacen que las blockchains sean una tecnología altamente segura y confiable para la gestión de datos y transacciones. Sin embargo, la seguridad en blockchain no es un asunto puramente técnico; también depende en gran medida de las acciones y precauciones de los usuarios para mantener la integridad de la tecnología y la confianza en su uso.

4.2.4. Adopción de Criptomonedas en Colombia.

La universidad del externado resaltó en su portal de noticias una publicación realizada por Criptonoticias, la cual indicaba que Colombia resultó el tercer país con mayor crecimiento de propietarios de bitcoin (BTC) y otras criptomonedas a nivel mundial.[65] El interés en las criptomonedas, había crecido entre la población colombiana, la Revista Forbes de Colombia la cual es un medio especializado en temas de negocios y finanzas indicó por medio de un artículo que Colombia se ubica en la novena posición en esta materia entre 154 países, siendo la segunda nación de América Latina en el ranking según un estudio de Chainalysis,[66] adicional se

[64] CLARKE, Anthony. La tecnología Blockchain mejora la transparencia de las organizaciones benéficas, pero ¿es adecuada para todas? Cointelegraph [página web]. (20, octubre, 2023). [Consultado el 14, septiembre, 2023]. Disponible en Internet: <https://es.cointelegraph.com/news/blockchain-charity-transparency-adoption>.

[65] COLOMBIA ES el tercer país con mayor crecimiento en adopción de criptomonedas en el mundo - Departamento de Derecho Financiero y Bursátil [Anónimo]. Departamento de Derecho Financiero y Bursátil [página web]. [Consultado el 26, septiembre, 2023]. Disponible en Internet: <https://observatoriofinancieroybursatil.uexternado.edu.co/colombia-es-el-tercer-pais-con-mayor-crecimiento-en-adopcion-de-criptomonedas-en-el-mundo/#:~:text=enero%20de%202022-,Colombia%20es%20el%20tercer%20país%20con%20mayor%20crecimiento%20en%20adopción,países%20latinoamericanos%20con%20mayor%20adopción.>.

[66] COLOMBIA, EN el 'top' 10 de países con mayor adopción de criptomonedas [Anónimo]. Forbes Colombia [página web]. [Consultado el 26, septiembre, 2023]. Disponible en Internet:

resalta que la adopción de este tipo de monda se debe a las plataformas de intercambio (exchange) los cuales son el lugar más popular para almacenar sus criptomonedas. El 60% de los usuarios las mantiene allí. Esto se debió en parte a la volatilidad de las monedas fiduciarias locales y a la búsqueda de alternativas de inversión.

La popularidad de la adopción de criptomonedas en Colombia ha experimentado un crecimiento notable en los últimos años, la inestabilidad económica es un factor significativo. Colombia, como muchos otros países de América Latina, ha enfrentado desafíos económicos, como la inflación y la devaluación de su moneda local. Las criptomonedas, especialmente Bitcoin, se perciben como una forma de resguardar el valor de los activos en un entorno económico incierto. Los colombianos han recurrido a las criptomonedas como una reserva de valor más estable en comparación con el peso colombiano. Según datos entregados por Colombia Fintech, en el país se conciben transacciones con criptomonedas por $70.000 millones mensuales y se han rastreado más de 600 sitios en los que se pueden comprar y vender.[67] Este tipo de comercio para criptomonedas brindan una forma de participar en el sistema financiero global sin necesidad de una cuenta bancaria, lo que puede tener un impacto positivo en la inclusión financiera.

<https://forbes.co/2021/03/02/economia-y-finanzas/colombia-en-el-top-10-de-paises-con-mayor-adopcion-de-criptomonedas>.

[67] LAS CRIPTOMONEDAS mueven $70.000 millones en transacciones en Colombia [Anónimo]. Semana.com Últimas Noticias de Colombia y el Mundo [página web]. (12, julio, 2022). [Consultado el 26, septiembre, 2023]. Disponible en Internet: <https://www.semana.com/economia/capsulas/articulo/las-criptomonedas-mueven-70000-millones-en-transacciones-en-colombia/202226/>.

4.2.5. Análisis de riesgos

La creación de un análisis de riesgo específico para Blockchain y Criptomonedas en Colombia es esencial para proteger los intereses de los ciudadanos, promover el crecimiento económico y tecnológico y garantizar una adopción segura y responsable de estas innovadoras tecnologías. Este análisis no solo es una herramienta útil, sino una necesidad imperativa para abordar los desafíos emergentes en el universo digital.

A medida que más colombianos participan en el mundo de las criptomonedas, es fundamental garantizar su seguridad financiera y la protección de sus inversiones. Un análisis de riesgo proporciona información valiosa sobre las amenazas potenciales, como estafas y fraudes, permitiendo a los usuarios tomar decisiones informadas y proteger sus activos. Por ello, las entidades implementan departamentos de gestión del riesgo que se encargan de analizar, evaluar y diseñar planes para mitigar los riesgos previstos en la implementación de marcos de trabajo basados en bloques de cadenas.[68]

Las criptomonedas pueden ser utilizadas en actividades ilícitas, como el lavado de dinero y la financiación del terrorismo. Un análisis de riesgo puede ayudar a diseñar estrategias efectivas para prevenir y combatir estos delitos financieros, lo que es fundamental para cumplir con las regulaciones nacionales e internacionales. Colombia, al igual que otros países, está considerando la regulación de las criptomonedas.

[68] IC Y Blockchain: retos y riesgos - OpenMind [Anónimo]. OpenMind [página web]. [Consultado el 19, septiembre, 2023]. Disponible en Internet: <https://www.bbvaopenmind.com/tecnologia/futuro/ic-y-blockchain-retos-y-riesgos/>.

4.3 MARCO HISTÓRICO

El blockchain es una tecnología que ha revolucionado la forma en que se entiende y se gestionan los registros digitales y representan una historia de innovación y avance tecnológico, cuyos inicios se remontan antes del surgimiento de Bitcoin, es decir, que sus orígenes se sitúan en la década de 1980, cuando se buscaban soluciones para garantizar la integridad y la inmutabilidad de los registros digitales.

Con el tiempo, el blockchain se ha convertido en una tecnología transformadora que se aplica en una variedad de industrias, desde la cadena de suministro y la atención médica hasta la gestión de identidad y el voto electrónico. Grandes empresas e instituciones financieras han comenzado a adoptar blockchain para mejorar la eficiencia y la seguridad en sus operaciones.

4.3.1. El Libro Blanco de Bitcoin (2008)

Sin embargo, el concepto del blockchain tal como se conoce hoy, se hizo realidad en 2008 con la creación de la moneda Bitcoin por una figura enigmática conocida como Satoshi Nakamoto.[69] El objetivo del proyecto Bitcoin era garantizar la seguridad, la transparencia y la privacidad entre los usuarios, dentro de un contexto donde un puñado de empresas controlaban la industria de Internet, a través de servidores de almacenamiento y gestión de datos particulares de clientes.[70] Este

[69] EL WHITEPAPER de Bitcoin ha sido traducido a más de 40 idiomas [Anónimo]. Bit2Me News | Noticias cripto, Blockchain, Ethereum [página web]. [Consultado el 19, octubre, 2023]. Disponible en Internet: <https://news.bit2me.com/whitepaper-de-bitcoin-traducido-a-mas-de-40-idiomas/#:~:text=En%20octubre%20de%202008,%20Satoshi,la%20autorización%20de%20una%20entidad>.

[70] BLOCKCHAIN ¿POR qué y cómo surge? Descúbrelo con Visualeo [Anónimo]. Visualeo [página web]. [Consultado el 19, octubre, 2023]. Disponible en Internet: <https://visualeo.com/blockchian-por-que-y-como-surge/#:~:text=Blockchain%20surge%20en%202008,%20dentro,sistema%20de%20seguridad%20prácticamente%20impenetrable.>.

fue un documento técnico que describió por primera vez el concepto y el funcionamiento de Bitcoin y su tecnología subyacente, el blockchain. En esencia, el Libro Blanco de Bitcoin es un documento que establece los fundamentos de una moneda digital descentralizada y cómo se resuelven los problemas de doble gasto en transacciones digitales. Proporciona la base teórica para la creación de Bitcoin y marcó el inicio de la revolución de las criptomonedas.

4.3.2. Creación de Bitcoin (2009)

En enero de 2009, se lanzó la red de Bitcoin, que implementó el primer blockchain funcional como el registro público de todas las transacciones de Bitcoin. Este evento marcó el inicio de la era del blockchain, lo cual supuso el origen de las criptomonedas, proporcionando a los ciudadanos un medio de pago que posibilite la ejecución de transferencias de valor rápidas, a bajo costo y que, además, no pueda ser controlado ni manipulado por gobiernos, bancos centrales o entidades financieras.[71] De esta manera brindó un nuevo enfoque para transferir valor en línea, eliminando la necesidad de intermediarios, como bancos, funcionando por medio de una red descentralizada, donde las transacciones se registran en un libro de contabilidad público llamado blockchain. Este evento revolucionario cambió la forma en que las personas ven y utilizan el dinero en el mundo digital y sirvió como punto de partida para la expansión de las criptomonedas y la tecnología blockchain en todo el mundo.

[71] QUÉ ES Bitcoin: origen, usos, ventajas y riesgos [Anónimo]. LISA Institute [página web]. [Consultado el 19, octubre, 2023]. Disponible en Internet: <https://www.lisainstitute.com/blogs/blog/que-es-bitcoin-origen-usos-ventajas-riesgos#:~:text=En%20enero%20de%202009%20entró,divisas%20como%20medio%20de%20pago.>.

4.3.3. Expansión del Uso de Blockchain (2010s)

Teniendo en cuenta que se generó esta expansión, la moneda de Bitcoin ganaba cada vez más atracción y la tecnología blockchain se aplicaba a otras áreas, como contratos inteligentes, es cuando en el 2013, esto llevó a un desarrollador canadiense, Vitalik Buterin, a proponer una nueva plataforma que permitiría una aplicación descentralizada para iniciar una nueva era de transacciones online. [72] El cual formalizo su lanzamiento en 2015 y permitió la creación de contratos inteligentes, lo que amplió significativamente las posibilidades de la tecnología blockchain.

BitcoinStore fue una de las primeras empresas en demostrar que las criptomonedas en seguida una empresa española llamada **Coinffeine**. Aporto junto con sus cuatro fundadores a bitcoins un valor de más de 3.000 euros almacenados en un cheque de papel verificado ante notario, creando así un precedente para las empresas que se quieran constituir de esta manera podían utilizarse de manera práctica para realizar transacciones comerciales en la vida cotidiana.[73] Su enfoque en la adopción de Bitcoin como método de pago contribuyó en el camino para la creciente aceptación de las criptomonedas en el mundo de los negocios.

Desde entonces, muchas otras empresas han seguido su ejemplo y la adopción de criptomonedas como Bitcoin en transacciones comerciales ha aumentado significativamente en todo el mundo. Empresas como Microsoft, Expedia y

[72] LA HISTORIA de Ethereum | Plus500 [Anónimo]. Online-CFD-Handel | Mit den Märkten handeln | Plus500 [página web]. [Consultado el 19, octubre, 2023]. Disponible en Internet: <https://www.plus500.com/es/Instruments/ETHUSD/The-History-of-Ethereum~4#:~:text=Creación%20de%20Ethereum&text=En%202015,%20después%20de%20una,sistema%20para%20abril%20de%202020.>.

[73] EL CONFIDENCIAL - El diario de los lectores influyentes [Anónimo]. elconfidencial.com [página web]. [Consultado el 27, septiembre, 2023]. Disponible en Internet: <https://www.elconfidencial.com/>.

Overstock.com también comenzaron a aceptar Bitcoin y otras criptomonedas como método de pago en sus plataformas.

En el 2017 fue el año del bitcoin en Colombia, según los reportes de sitios especializados que monitorean las transacciones hechas con la criptomoneda. De hecho, uno de los sitios más grandes de compra y venta de bitcoins de persona a persona, Local bitcoins, indicó que las transacciones hechas con pesos colombianos crecieron 1.200% durante 2017.[74]

Colombia ha visto el surgimiento de startups y proyectos basados en blockchain que abordan diversos sectores, como la cadena de suministro, la identidad digital y la educación. Estos proyectos están demostrando el potencial de la tecnología blockchain en la resolución de problemas locales.

4.4 ANTECDENTES O ESTADO ACTUAL

La adopción de criptomonedas y la conciencia de la tecnología blockchain han ido en aumento en Colombia. Más ciudadanos están invirtiendo en criptomonedas y empresas locales han comenzado a aceptar Bitcoin y otras criptomonedas como forma de pago, Colombia se destaca como uno de los países líderes en adopción de criptomonedas, pero lo que lo hace más interesante, es su ecosistema que lo distingue como el único país de la región que alberga a una gran comunidad conformada por desarrolladores con gran talento, startups innovadores y un gobierno e instituciones abiertas a adoptar esta tecnología. Esta singular

[74] CÓMO COLOMBIA se convirtió en el país de América Latina en el que más crece la compra y venta de bitcoins - BBC News Mundo [Anónimo]. BBC News Mundo [página web]. [Consultado el 10, octubre, 2023]. Disponible en Internet: <https://www.bbc.com/mundo/noticias-america-latina-43219365#:~:text=2017%20fue%20el%20año%20del,transacciones%20hechas%20con%20la%20criptomoneda.>.

combinación refleja el inmenso potencial de crecimiento que encierra el ecosistema local.

Se realizó en Bogotá la séptima edición del Blockchain Summit Latam 2023. Un evento que reunió durante tres días a los principales actores del ecosistema blockchain y cripto en América Latina y en el que los asistentes tuvieron la oportunidad de explorar el potencial de esta tecnología en diversas áreas, desde el gobierno hasta los servicios financieros, el comercio internacional, las finanzas descentralizadas y mucho más.[75]

4.4.1. Educación y Concienciación

La educación y la concienciación sobre criptomonedas y blockchain son esenciales en un mundo, donde estas tecnologías disruptivas están tomando cada vez más relevancia. Ya seas un principiante que recién comienza a explorar el mundo de las criptomonedas o un entusiasta experimentado que busca mantenerse al tanto de las últimas novedades, la educación y la concienciación son clave para comprender y utilizar estas innovaciones de manera segura y efectiva.

Antes de sumergirse en el mundo de las criptomonedas y la tecnología blockchain, es crucial comprender los conceptos fundamentales, como lo que es una criptomoneda, cómo funcionan las transacciones en una cadena de bloques y qué es una billetera digital. La educación proporciona las bases necesarias para participar de manera informada. Actualmente Binance Colombia anunció que colaborará con la Universidad de los Andes (Uniandes) para crear programas educativos para estudiantes y profesores universitarios sobre la Web 3.0 y la

[75] BLOCKCHAIN SUMMMIT Colombia 2023: Abriendo puertas a la transformación tecnológica - Prensario Tila [Anónimo]. Prensario Tila [página web]. [Consultado el 18, octubre, 2023]. Disponible en Internet: <https://prensariotila.com/blockchain-summmit-colombia-2023-abriendo-puertas-a-la-transformacion-tecnologica/>.

tecnología blockchain en el país, a través de Binance Academy.[76] De esta manera les permitirá asistir a conferencias y eventos es una excelente manera de conectarse con expertos y mantenerse actualizado sobre los desarrollos más recientes en el espacio de criptomonedas y blockchain.

4.4.2. Iniciativas Gubernamentales

Algunos gobiernos están lanzando iniciativas para educar a los ciudadanos sobre las criptomonedas y la tecnología blockchain. Esto a menudo se hace en un esfuerzo por promover un uso seguro y legal de las criptomonedas, así como para abordar posibles preocupaciones sobre el lavado de dinero y la evasión fiscal.

Las policías y fiscalías de 17 países de América Latina y la Unión Europea se unieron para concientizar sobre las estafas más comunes detectadas en las inversiones con criptomonedas, mediante una campaña de comunicación y sensibilización y la red contra el Cibercrimen CibEL@.[77]

Adicional, el gobierno colombiano ha mostrado interés en apoyar a los startups tecnológicos, incluidas aquellas que trabajan en proyectos basados en blockchain. Los programas de apoyo a emprendedores y el financiamiento a través de fondos de inversión respaldados por el gobierno son ejemplos de medidas destinadas a fomentar la innovación tecnológica.

---

[76] BINANCE COLOMBIA Y la Universidad de los Andes lanzarán cursos sobre Web3 [Anónimo]. BeInCrypto [página web]. [Consultado el 18, octubre, 2023]. Disponible en Internet: <https://es.beincrypto.com/binance-colombia-universidad-andes-lanzaran-cursos-web3/>.

[77] CAMPAÑA #FAKECOINS: estafas con criptomonedas [Anónimo]. Policía De Investigaciones [página web]. [Consultado el 19, octubre, 2023]. Disponible en Internet: <https://www.pdichile.cl/centro-de-prensa/detalle-prensa/2022/03/30/campaña-fakecoins-estafas-con-criptomonedas>.

4.5 MARCO CIENTÍFICO O TECNOLÓGICO

4.5.1. Exploración de las amenazas cibernéticas y las tácticas maliciosas.

Las criptomonedas han revolucionado la forma en que se percibe y utiliza el dinero, pero también han dado lugar a un conjunto de amenazas emergentes en el espacio cibernético. Los ataques de cryptomining, también conocidos como cryptojacking, funcionan mediante la instalación de malware que utiliza la capacidad de procesamiento de un ordenador para minar criptomonedas sin el consentimiento o el conocimiento del propietario. Sin duda, esto se han convertido en una de las tendencias principales y peligrosas dentro del mercado.[78] Es esencial mantener una fuerte educación en seguridad cibernética, utilizar billeteras seguras, habilitar la autenticación de dos factores, verificar siempre la autenticidad de los sitios web y las comunicaciones relacionadas con criptomonedas. Para ello, se aborda las siguientes amenazas emergentes:

- **Estafas de inversión y esquemas Ponzi:** Los esquemas de Ponzi se conocen por Carlo Ponzi, un famoso delincuente de origen italiano que estafó a muchas personas en los años 20 en Estados Unidos.[79] Los estafadores a menudo prometen rendimientos exorbitantes a través de inversiones en criptomonedas. Estos esquemas suelen ser fraudulentos y se basan en el principio de utilizar los fondos de los nuevos inversores para pagar a los inversores anteriores, creando así la ilusión de ganancias. Los esquemas Ponzi en criptomonedas pueden ser difíciles de detectar debido a la falta de regulación y transparencia en el mercado.

[78] LAS AMENAZAS emergentes en seguridad: Cryptomining, SASE - PrensarioHub [Anónimo]. PrensarioHub [página web]. [Consultado el 27, septiembre, 2023]. Disponible en Internet: <https://www.prensariohub.com/las-amenazas-emergentes-en-seguridad-cryptomining-

[79] ¿CÓMO FUNCIONA un esquema Ponzi? [Anónimo]. BBVA NOTICIAS [página web]. [Consultado el 27, septiembre, 2023]. Disponible en Internet: <https://www.bbva.com/es/como-funciona-un-sistema-ponzi-conocelo-para-protegerte/>.

- **Phishing y suplantación de identidad:** El banco BBVA informa que este tipo de ataque pertenece a una categoría de técnica de ingeniería social que consiste en el envío de correos electrónicos que suplantan la identidad de compañías u organismos públicos y solicitan información personal y bancaria al usuario.[80] Los atacantes envían correos electrónicos y mensajes falsos que parecen provenir de intercambios de criptomonedas legítimos o billeteras, con el objetivo de engañar a las personas para que divulguen sus claves privadas o información de inicio de sesión. Una vez que obtienen acceso a estas claves, pueden robar los activos de la víctima.

- **Ataques de doble gasto:** En algunos casos, los atacantes pueden intentar gastar la misma criptomoneda dos veces al aprovechar una falla en la confirmación de la red. Este tipo de ataque es más común en criptomonedas con menor poder de procesamiento y los atacantes pueden beneficiarse al gastar los fondos y luego revertir la transacción antes de que se confirme.

- **Malware de minería de criptomonedas o cryptojacking:** Los hackers pueden infectar dispositivos de usuarios con malware diseñado para minar criptomonedas sin su consentimiento. La empresa de telecomunicaciones Movistar detalla que está es una amenaza emergente de Internet que se oculta en un ordenador o en un dispositivo móvil y utiliza los recursos de la máquina para “extraer” diversas formas de monedas digitales conocidas como criptomonedas.[81] Esto puede ralentizar significativamente el rendimiento de la computadora y aumentar el consumo de energía.

---

[80] ESPAÑA, BBVA. ¿Qué es el phishing y cuáles son sus consecuencias? Banco BBVA - Productos financieros para personas y empresas | BBVA [página web]. (9, marzo, 2020). [Consultado el 26, septiembre, 2023]. Disponible en Internet: <https://www.bbva.es/finanzas-vistazo/ciberseguridad/ataques-informaticos/que-es-el-phishing-y-cuales-son-sus-consecuencias.html>.

[81] CRYPTOJACKING – ¿Qué es y cómo funciona? | Malwarebytes [Anónimo]. Malwarebytes [página web]. [Consultado el 26, septiembre, 2023]. Disponible en Internet: <https://es.malwarebytes.com/cryptojacking/#:~:text=El%20cryptojacking%20es%20una%20forma, monedas%20online%20como%20el%20bitcoin.>.

- **Ransomware que exige criptomonedas:** La empresa ESET reconoce que este tipo de ataque pertenece a una categoría de código malicioso diseñada para secuestrar el poder de cómputo inactivo del dispositivo de la víctima y usarlo para minar criptomonedas. No se solicita a los usuarios su consentimiento para tal actividad; de hecho, por lo general las víctimas desconocen lo que está sucediendo en su equipo en segundo plano.[82] Los ataques de ransomware han evolucionado para exigir pagos en criptomonedas, ya que proporcionan un grado de anonimato para los atacantes. Las víctimas se ven obligadas a pagar un rescate en criptomonedas para recuperar sus datos o sistemas.

- **Robo de billeteras y claves privadas:** Los delincuentes pueden robar claves privadas de billeteras digitales o utilizar técnicas de ingeniería social para convencer a las personas de que compartan sus claves privadas. Una vez que tienen acceso a estas claves, pueden vaciar las billeteras de las víctimas.

- **Ataques de ingeniería social:** Los atacantes pueden utilizar tácticas de ingeniería social para engañar a las personas y obtener acceso a sus cuentas o fondos de criptomonedas. Esto puede incluir la suplantación de identidad, la manipulación emocional o la explotación de la confianza.

[82] MALWARE DE extracción de criptomonedas (cryptojacking): qué es y cómo protegerse | ESET [Anónimo]. Malware Protection & Internet Security | ESET [página web]. [Consultado el 26, septiembre, 2023]. Disponible en Internet: <https://www.eset.com/co/malware-extraccion-cryptomonedas/>.

4.5.2. Soluciones de Seguridad Emergentes

La seguridad en el mundo de las criptomonedas es una preocupación constante, en donde la evolución de las tecnologías y soluciones de seguridad es esencial para proteger los activos y fomentar la confianza en esta industria en crecimiento, bridando enfoques y tecnologías avanzadas que se desarrollan para abordar nuevas amenazas y desafíos en el entorno digital. Estas soluciones buscan mejorar la protección de datos, sistemas y activos digitales y suelen ser respuestas a amenazas cibernéticas en constante evolución. El señor Jaime Chanaga,de CISO en Fortinet para Latinoamérica indica que el panorama de ciber amenazas continúa evolucionando y se predice que el 2023 traerá consigo viejas y nuevas tácticas de intrusión. Los CIOs y CISOs se enfrentan a la tarea de superar importantes retos al tiempo que trabajan para manejar las iniciativas que se han vuelto críticas para la operación de un negocio como asegurar los dispositivos,[83] por ello se incluyen los siguientes ejemplos de tecnologías como autenticación multifactor, contratos inteligentes seguros en blockchain, herramientas de detección de amenazas avanzadas y protocolos de privacidad en criptomonedas. Estas soluciones son esenciales para mantener la seguridad en un mundo digital en constante cambio.

[83] LAS SOLUCIONES de ciberseguridad que deberían priorizar las empresas este 2023 - Prensario Tila [Anónimo]. Prensario Tila [página web]. [Consultado el 26, septiembre, 2023]. Disponible en Internet: <https://prensariotila.com/las-soluciones-de-ciberseguridad-que-deberian-priorizar-las-empresas-este-2023/>.

4.6 MARCO LEGAL

4.6.1. Regulación en Colombia

Es importante señalar que, si bien las criptomonedas tienen ventajas significativas, también están asociadas con riesgos, incluida la volatilidad de precios y la falta de regulación en algunos lugares. Por lo tanto, las personas deben educarse y tomar decisiones financieras informadas al considerar la adopción de criptomonedas. En la actualidad en el Senado de la República de Colombia se tiene el proyecto de ley 268 que define las criptomonedas como un "activo digital" que puede usarse para intercambiar bienes y servicios, pero no las considera ni moneda de curso legal, ni divisas ni títulos representativo de moneda legitima del país.[84]

De igual manera la Superintendencia Financiera de Colombia, que es la entidad reguladora financiera del país, había emitido algunas advertencias sobre los riesgos asociados con las criptomonedas y la necesidad de ser cauteloso al invertir en ellas. También ha llevado a cabo discusiones en el Congreso de la República sobre la necesidad de establecer una regulación adecuada. Los Senadores Gustavo Moreno y Julián López impulsaron la iniciativa y proyecto de ley No. 267 de 2022, "Por la cual se regulan los Servicios de Intercambio de Criptoactivos ofrecidos a través de las Plataformas de Intercambio de Criptoactivos", la iniciativa busca establecer un marco normativo para el uso de las monedas virtuales o criptomonedas y sus formas de transacción en Colombia, con el propósito de establecer una clara regulación para los proveedores de servicios de activos virtuales (PSAV) y alcanzar una

[84] GUÍA PRÁCTICA sobre el tratamiento legal de las Criptomonedas en Colombia: Recomendaciones y reflexiones [Anónimo]. Centro de Estudios Regulatorios [página web]. [Consultado el 26, septiembre, 2023]. Disponible en Internet: <https://www.cerlatam.com/publicaciones/guia-practica-sobre-el-tratamiento-legal-de-las-criptomonedas-en-colombia-recomendaciones-y-reflexiones/#:~:text=El%20proyecto%20de%20ley%20268%20de%202019.,de%20moneda%20de%20curso%20legal.>.

protección de los consumidores.[85] Es vital tener una entidad reguladora en Colombia para las criptomonedas porque brinda protección al consumidor, previene actividades ilícitas, garantiza la seguridad del mercado y fomenta la adopción responsable.

4.6.2. Legislación Colombiana

El gobierno colombiano había estado evaluando la necesidad de regulaciones para abordar cuestiones como el lavado de dinero y la protección del consumidor en el contexto de las criptomonedas.

La Superintendencia Financiera de Colombia emitió comunicados advirtiendo sobre los riesgos asociados con las inversiones en criptomonedas. Afirmaron que las criptomonedas no están respaldadas por el gobierno colombiano y que no están reguladas por las autoridades financieras del país y considera que las criptomonedas son un activo intangible y, por lo tanto, sujeto a impuestos sobre las ganancias de capital.[86] Las transacciones con criptomonedas debían registrarse y declararse en la declaración de impuestos.

[85] LEGALIDAD DE las Criptomonedas: Avance significativo en la economía digital de Colombia - Blog Jurídico - TECH [Anónimo]. Blog Jurídico - TECH [página web]. [Consultado el 26, septiembre, 2023]. Disponible en Internet: <https://telecomunicaciones.uexternado.edu.co/legalidad-de-las-criptomonedas-avance-significativo-en-la-economia-digital-de-colombia/#:~:text=Más%20adelante,%20el%20presidente%20Luiz,junio%20del%202023[5].>.

[86] ESTAS SON las siete dudas legales sobre el uso de los criptoactivos y su regulación [Anónimo]. Noticias de Abogados, bufetes, jurisprudencia, avisos de ley, de Colombia| Asuntoslegales.com.co [página web]. [Consultado el 19, octubre, 2023]. Disponible en Internet: <https://www.asuntoslegales.com.co/actualidad/estas-son-las-siete-dudas-legales-sobre-el-uso-de-los-criptoactivos-y-su-regulacion-3155325>.

Figura 2. Regulación de las criptomonedas

Fuente: Argote (2021). Estado legal de las criptomonedas en Colombia. Imagen tomada de: https://www.asuntoslegales.com.co/actualidad/estas-son-las-siete-dudas-legales-sobre-el-uso-de-los-criptoactivos-y-su-regulacion-3155325

4.6.3. Regulaciones en Ciberseguridad

La regulaciones, leyes y normatividades en ciberseguridad desempeñan un papel crítico en la protección de la sociedad y la economía en un mundo cada vez más interconectado. Sin estas medidas, la sociedad estaría expuesta a un mayor riesgo de delitos cibernéticos y a la vulnerabilidad de los sistemas digitales. La ciberseguridad es una responsabilidad compartida que requiere de una sólida base legal para garantizar la seguridad en el ciberespacio.

- **Ley 1273 de 2009 (Ley de Delitos Informáticos):** Es reconocida principalmente por la preservación integralmente de los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.[87] De esta manera la ley define y penaliza una serie de delitos informáticos, como el acceso no autorizado a sistemas informáticos, la interceptación de datos y la destrucción de datos, estableciendo sanciones para quienes cometan estos delitos.

- **Ley 1581 de 2012 (Ley de Protección de Datos Personales):** Reconoce y protege el derecho que tienen todas las personas a conocer, actualizar y rectificar la información recogida sobre ellas en bases de datos o archivos que sean susceptibles de tratamiento por entidades de naturaleza pública o privada.[88] Aunque no se trata de una ley de ciberseguridad en el sentido tradicional, esta ley regula la protección de datos personales y establece requisitos para el tratamiento de esta información. Impone obligaciones a las organizaciones que manejan datos personales y busca proteger la privacidad de los individuos.

- **Decreto 620 de 2020:** El Ministerio de Tecnologías de la Información y las Comunicaciones expidió el Decreto para establecer lineamientos generales para el uso y operación de los servicios ciudadanos digitales.[89] Este decreto

[87] LEY 1273 de 2009 -Legislacion Colombiana Lexbase [Anónimo]. INFORMACION JURIDICA, BASE DE DATOS ESPECIALIZADA , BASE DE DATOS JURIDICA LEXBASE - COLOMBIA [página web]. [Consultado el 20, octubre, 2023]. Disponible en Internet: <https://www.lexbase.co/lexdocs/indice/2009/l1273de2009#:~:text="%20LEY%201273%20DE%20 2009%20(enero,y%20las%20comunicaciones,%20entre%20otras>.

[88] POLÍTICA DE Protección de Datos Personales - Ministerio de Ambiente y Desarrollo Sostenible [Anónimo]. Ministerio de Ambiente y Desarrollo Sostenible [página web]. [Consultado el 20, octubre, 2023]. Disponible en Internet: <https://www.minambiente.gov.co/politica-de-proteccion-de-datos-personales/#:~:text=Ley%20de%20Protección%20de%20Datos,de%20naturaleza%20pública%20o %20privada.>.

[89] COLOMBIA: DECRETO 620 de 2020 - Uso y operación de los servicios ciudadanos digitales [Anónimo]. Dentons Cardenas & Cardenas - Home [página web]. [Consultado el 19, octubre, 2023]. Disponible en Internet: <https://dentons.cardenas-cardenas.com/es/insights/articles/2020/may/7/colombia-decree-620-of-2020-use-and-operation-of-

regula la seguridad de la información y establece directrices para la implementación de medidas de ciberseguridad en las entidades públicas y privadas. También define las obligaciones de notificación de incidentes de seguridad.

- **Decreto 1074 de 2015:** Este decreto reglamenta la Ley 1581 de 2012 y establece disposiciones específicas sobre la protección de datos personales, incluyendo la creación de registros de actividades de tratamiento y la notificación de brechas de seguridad.[90]

- **Circulares de la Superintendencia Financiera:** La Superintendencia Financiera de Colombia ha emitido varias circulares que establecen lineamientos específicos para las entidades financieras en materia de seguridad de la información y ciberseguridad. Estas circulares son relevantes para las instituciones financieras en el país.

4.6.4 Normatividad y Estándar

- **ISO 27001:** es un estándar internacional que establece los requisitos para la implementación, mantenimiento y mejora continua de un Sistema de Gestión de la Seguridad de la Información (SGSI). Este sistema se utiliza para proteger la confidencialidad, integridad y disponibilidad de la información. La norma proporciona un marco para la seguridad de la información que ayuda

digital-citizen-services#:~:text=servicios%20ciudadanos%20digitales-,Colombia:%20Decreto%20620%20de%202020%20-%20Uso%20y%20operación,de%20los%20servicios%20ciudadanos%20digitales&text=El%20Ministerio%20de%20Tecnologías%20de,de%20los%20servicios%20ciudadanos%20digitales.>.

[90] DECRETO 1074 de 2015 [Anónimo]. MINTIC [página web]. [Consultado el 19, octubre, 2023]. Disponible en Internet: <https://www.mincit.gov.co/ministerio/normograma-sig/procesos-misionales/facilitacion-del-comercio-y-defensa-comercial/decretos/2015/decreto-1074-de-2015-1.aspx>.

a las organizaciones a identificar y gestionar sus riesgos de seguridad de la información de manera efectiva.[91] Muchas organizaciones en Colombia optan por certificarse bajo este estándar como parte de sus esfuerzos de seguridad, ayudando a identificar y abordar las vulnerabilidades y amenazas a la seguridad de la información, mejorando así la seguridad de los activos digitales.

- **NIST Cybersecurity Framework:** Aunque es un estándar de ciberseguridad desarrollado en los Estados Unidos, el Marco de Ciberseguridad del NIST se utiliza ampliamente en todo el mundo y puede ser referente para organizaciones colombianas que deseen establecer políticas de ciberseguridad. Es una agencia que promueve la innovación mediante el fomento de la ciencia, los estándares y la tecnología de la medición, consta de estándares, pautas y mejores prácticas que ayudan a las organizaciones a mejorar su gestión de riesgos, tiene una flexibilidad que le permite integrarse con los procesos de seguridad existentes dentro de cualquier organización, en cualquier industria.[92]

- **COBIT (Control Objectives for Information and Related Technologies):** es un marco de gestión de TI y gobierno corporativo que incluye pautas y buenas prácticas para la gestión de la seguridad de la información, ha evolucionado desde una herramienta para auditoría a un marco de buen gobierno de TIC,[93] ayuda a cubrir las necesidades fiduciarias, de calidad y

[91] ¿QUÉ ES la norma ISO 27001 y para qué sirve? [Anónimo]. GlobalSuite Solutions [página web]. [Consultado el 20, octubre, 2023]. Disponible en Internet: <https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-27001-y-para-que-sirve/>.
[92] ¿QUÉ ES el marco de ciberseguridad del NIST? | IBM [Anónimo]. IBM in Deutschland, Österreich und der Schweiz | IBM [página web]. [Consultado el 21, octubre, 2023]. Disponible en Internet: <https://www.ibm.com/mx-es/topics/nist#:~:text=El%20Instituto%20Nacional%20de%20Estándares,la%20tecnología%20de%20la%20medición.>.
[93] BLOG DE CEUPE. ¿Qué es COBIT? Ceupe [página web]. (27, noviembre, 2018). [Consultado el 21, octubre, 2023]. Disponible en Internet: <https://www.ceupe.com/blog/que-es-cobit.html>.

seguridad de las organizaciones, proporcionando siete criterios de información que se pueden utilizar para definir genéricamente lo que la empresa requiere, por lo que muchas empresas en Colombia adoptan COBIT para mejorar la ciberseguridad.

- **ITIL (Information Technology Infrastructure Library):** es una guía de buenas prácticas para la gestión de servicios de tecnologías de la información ha sido elaborada para abarcar toda la infraestructura, desarrollo y operaciones de TI y gestionarla hacia la mejora de la calidad del servicio.[94] Por esta razón es esencial para garantizar que la gestión de servicios de TI sea eficiente, efectiva y alineada con los objetivos del negocio. Esto se traduce en una mejor calidad de los servicios de TI, la satisfacción del cliente y la capacidad de las organizaciones para enfrentar los desafíos tecnológicos en un mundo cada vez más digital.

[94] ¿QUÉ ES ITIL y para que sirve? [Anónimo]. GlobalSuite Solutions [página web]. [Consultado el 21, octubre, 2023]. Disponible en Internet: <https://www.globalsuitesolutions.com/es/que-es-itil-y-para-que-sirve/>.

5 UN MUNDO EN EVOLUCIÓN: DESAFÍO DE LA SEGURIDAD EN CRIPTOMONEDAS

En este capítulo, se explorarán las diferencias y se resaltará la necesidad de estrategias de seguridad específicas para enfrentar las amenazas emergentes en el ámbito de las criptomonedas y la seguridad digital en general.

Para ello, se examinarán las características únicas de las criptomonedas, su tecnología subyacente, así como las amenazas que han surgido entorno a su uso y adopción. Se compararán las amenazas tradicionales en seguridad digital, como el malware, la ingeniería social y otros ataques cibernéticos comunes. Al hacerlo, se espera proporcionar una visión más clara de cómo abordar la seguridad en un entorno digital diverso y en constante evolución.

5.1 CRIPTOMONEDAS Y SEGURIDAD DIGITAL: UNA COMPARATIVA DE AMENAZAS EMERGENTES Y TRADICIONALES

Es fundamental abordar estas temáticas con la finalidad de proteger activos financieros, fomentar la innovación tecnológica, preservar la privacidad y la seguridad de datos, construir confianza, mantener la estabilidad económica, prevenir delitos financieros y facilitar la regulación adecuada. Este enfoque es esencial en un mundo cada vez más digital y globalizado.

5.1.1. Metodología para la recolección de información

Al utilizar el análisis cuantitativo, este método permite recopilar datos numéricos de manera estructurada, lo que facilita su análisis y comparación, para obtener una visión clara de las percepciones y conocimientos de las personas sobre las criptomonedas, ya que permite identificar patrones y tendencias con precisión. Al tener opciones predefinidas en las respuestas, se asegura que los datos sean más fáciles de procesar estadísticamente, ayudando a generar conclusiones objetivas y confiables.

Las preguntas serán diseñadas para cubrir tres áreas principales:

- **Percepciones generales sobre las criptomonedas:** Estas preguntas buscarán conocer si los participantes confían o desconfían de las criptomonedas, si consideran que son seguras, entre otros factores.
- **Conocimiento sobre mitos comunes:** Se evaluará si los encuestados creen en ciertos mitos relacionados con las criptomonedas, como su uso exclusivo en actividades ilícitas o su supuesta falta de regulación.
- **Comprensión de los servicios ofrecidos:** Las preguntas medirán el nivel de conocimiento sobre las funcionalidades y servicios que las criptomonedas pueden ofrecer.

5.1.2. Importancia de distinguir entre amenazas emergentes

La importancia de distinguir entre amenazas emergentes y tradicionales en seguridad digital en el contexto de las criptomonedas radica en varios aspectos clave que afectan a individuos, organizaciones y la sociedad en su conjunto resaltan los siguientes factores:

- **Protección de Activos Financieros:** Las criptomonedas representan una forma de activo financiero que se basa en tecnología digital y blockchain. La pérdida o el robo de criptomonedas debido a amenazas emergentes puede tener un impacto económico significativo en individuos y organizaciones.

- **Innovación Tecnológica:** La tecnología de criptomonedas, como la cadena de bloques (blockchain), ha introducido innovaciones tecnológicas importantes. Las amenazas emergentes a menudo explotan estas innovaciones. Comprender estas amenazas es crucial para avanzar en la adopción y el desarrollo de tecnologías emergentes y garantizar su seguridad.

- **Privacidad y Seguridad de Datos:** Las criptomonedas requieren el almacenamiento de información personal y financiera sensible. Las amenazas emergentes pueden comprometer la privacidad y la seguridad de estos datos y es imperativo ético y legal salvaguardar esta información.

- **Confianza del Usuario:** La confianza de los usuarios es fundamental para la adopción generalizada de criptomonedas. Las amenazas emergentes, como estafas y ataques, pueden socavar esta confianza. Distinguir estas amenazas ayuda a construir una comunidad de usuarios más segura y confiable.

- **Economía Digital:** Las criptomonedas son un componente esencial de la economía digital global. La seguridad en este entorno es crucial para el funcionamiento eficiente de la economía digital y para evitar perturbaciones económicas.

- **Prevención de Delitos Financieros:** La falta de distinción entre amenazas emergentes y tradicionales puede dificultar la prevención y el enjuiciamiento

de delitos financieros relacionados con criptomonedas. La comprensión de las amenazas es esencial para aplicar la ley y prevenir actividades delictivas.

- **Regulación y Políticas Públicas:** Los gobiernos y las autoridades reguladoras están desarrollando políticas públicas y regulaciones relacionadas con las criptomonedas. Distinguir amenazas emergentes ayuda a las autoridades a diseñar regulaciones efectivas y proporcionar orientación a los usuarios y las empresas.

- **Inversión y Desarrollo Empresarial:** Empresas e inversionistas están explorando oportunidades en el espacio de las criptomonedas y la tecnología blockchain. La identificación de amenazas emergentes permite a estas partes interesadas tomar decisiones informadas y desarrollar estrategias de seguridad efectivas.

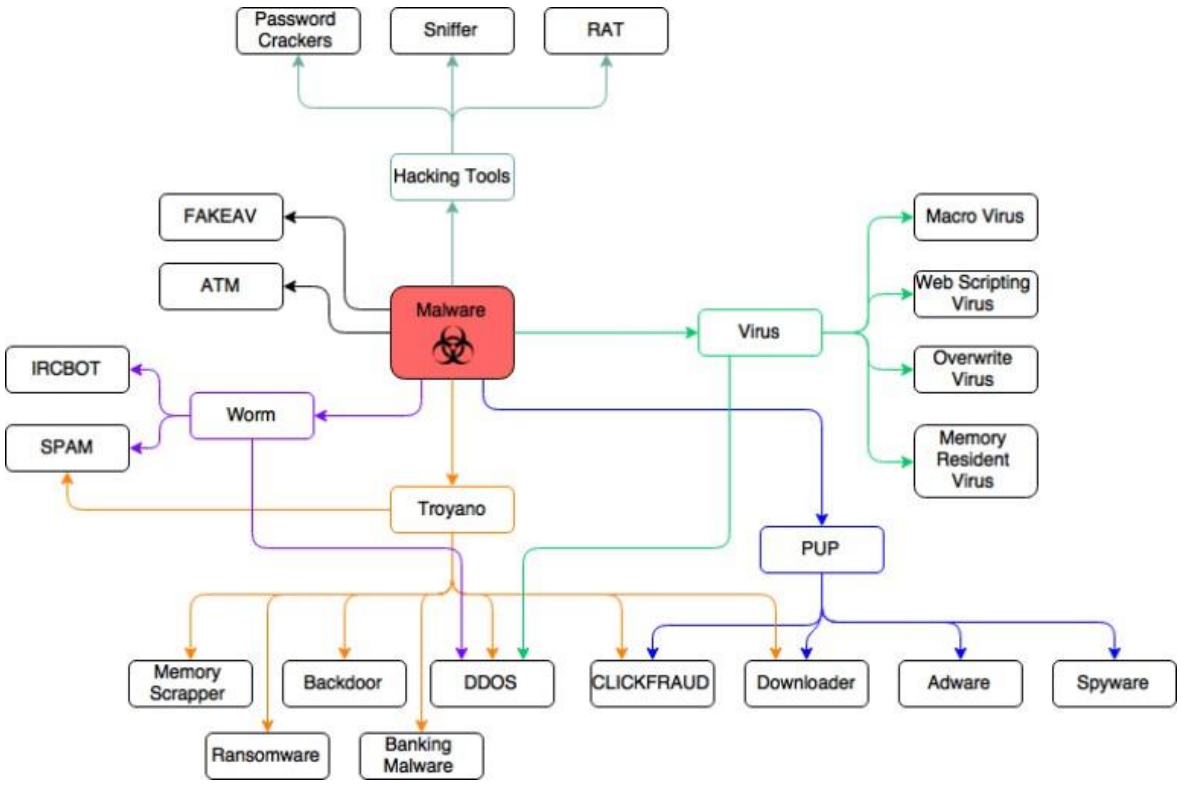
5.1.3. Amenazas Tradicionales en Seguridad Digital

Es todo lo que atenta contra la seguridad de la información de las personas. Los usuarios están expuestos a las amenazas cuando navegan por internet, utilizan servicios, hacen compras u otras actividades por medio de internet,[95] este tipo de ataques se han desarrollado y perfeccionado a lo largo del tiempo en el ámbito de la ciberseguridad. Estas amenazas son conocidas y bien documentadas y a menudo se basan en técnicas y métodos que han existido durante años. A continuación, se describen algunas de las amenazas tradicionales más comunes en seguridad digital:

[95] GUÍA PARA madres, padres, familias y docentes: amenazas en internet [Anónimo]. Argentina.gob.ar [página web]. [Consultado el 21, octubre, 2023]. Disponible en Internet: <https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/guia-para-madres-padres-docentes-amenazas-internet#:~:text=Es%20todo%20lo%20que%20atenta,actividades%20por%20medio%20de%20internet.>.

- **Malware (Software Malicioso):** es un término amplio que describe cualquier programa o código malicioso que sea dañino para los sistemas. [96] Están diseñados para infiltrarse o dañar, robar información confidencial o interrumpir su funcionamiento normal, por lo cual engloba varios tipos de software malicioso, como los que se observan en la siguiente imagen:

Figura 3. Tipos de malware



Fuente: Eduardo Ruiz Azofra (2015). Tipos de malware. Imagen tomada de: https://oa.upm.es/38772/1/PFC_EDUARDO_RUIZ_AZOFRA_2015.pdf

[96] ¿QUÉ ES el malware? Definición y cómo saber si está infectado | Malwarebytes [Anónimo]. Malwarebytes [página web]. [Consultado el 22, octubre, 2023]. Disponible en Internet: <https://es.malwarebytes.com/malware/>.

- **Phishing:** es una estrategia en la que los atacantes envían correos electrónicos malintencionados diseñados para estafar a sus víctimas. La idea consiste en que los usuarios revelen información financiera, credenciales del sistema u otros datos delicados.[97] Implica engañar a las personas para que divulguen información confidencial, como contraseñas, números de tarjetas de crédito o datos personales. Los atacantes suelen utilizar correos electrónicos o sitios web falsos que se asemejan a comunicaciones legítimas.

- **Ingeniería Social:** emplea técnicas de manipulación psicológica para obtener información confidencial de personas y empresas. Los ciberdelincuentes recopilan la información que compartimos en Internet, como son nuestros datos personales, la empresa para la que trabaja el usuario o sus costumbres, para ganar su confianza y obtener lo que buscan.[98] Esto puede incluir tácticas como el engaño, la persuasión y la explotación de la confianza de las personas, en la siguiente imagen se aprecia un ejemplo del funcionamiento:

Figura 4. Como funciona la Ingeniería social

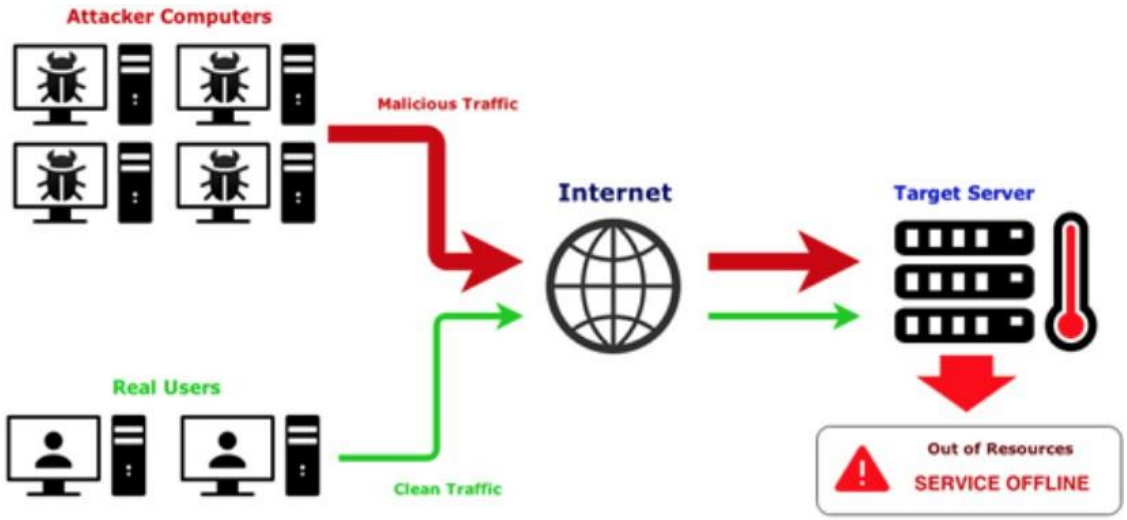
Fuente: Click-it. (2021). Como funciona la Ingeniería social. Imagen tomada de: https://click-it.es/ingenieria-social-que-es-y-como-prevenirla/

[97] ¿QUÉ ES phishing? - Definición, ejemplos de ataques y más | Proofpoint ES [Anónimo]. Proofpoint [página web]. [Consultado el 22, octubre, 2023]. Disponible en Internet: <https://www.proofpoint.com/es/threat-reference/phishing>.
[98] INGENIERÍA SOCIAL: qué es y cómo prevenirla | Click-IT | Servicios tecnológicos y de consultoría [Anónimo]. Click-IT | Servicios tecnológicos y de consultoría | [página web]. [Consultado el 22, octubre, 2023]. Disponible en Internet: <https://click-it.es/ingenieria-social-que-es-y-como-prevenirla/>.

- **Ataques de Fuerza Bruta:** son intentos de averiguar una contraseña o un nombre de usuario, o de encontrar una página web oculta o la clave utilizada para cifrar un mensaje, mediante un enfoque de prueba y error, con la esperanza de acertar.[99] Estos ataques son lentos, pero pueden ser efectivos si las contraseñas son débiles.

- **Ataques de Denegación de Servicio (DDoS):** son un tipo de ciberataque que intenta hacer que un sitio web o recurso de red no esté disponible al colapsar con tráfico malintencionado para que no pueda funcionar correctamente,[100] un atacante sobrecarga su objetivo con tráfico de Internet no deseado para que el tráfico normal no llegue a su destino previsto, lo que provoca la inaccesibilidad del servicio para usuarios legítimos.

Figura 5. Operación del ataque de DDoS



Fuente: Cudlayer (2018). Operación del ataque de DDoS. Imagen tomada de: https://nextvision.com/que-es-un-ataque-ddos-y-como-detenerlo/

[99] ¿QUÉ ES un ataque de fuerza bruta? [Anónimo]. latam.kaspersky.com [página web]. [Consultado el 22, octubre, 2023]. Disponible en Internet: <https://latam.kaspersky.com/resource-center/definitions/brute-force-attack>.
[100] ¿QUÉ ES un ataque DDoS? [Anónimo]. akamai [página web]. [Consultado el 22, octubre, 2023]. Disponible en Internet: <https://www.akamai.com/es/glossary/what-is-ddos>.

- **Adware:** es un tipo de programa publicitario malicioso. La primera es mostrar anuncios en el navegador o en el celular para que los autores puedan obtener ganancias y la segunda es recopilar información personal [101] o afectar negativamente el rendimiento.

- **Spyware (Programas Espía):** como un software diseñado para recopilar datos de un ordenador u otro dispositivo y reenviarlos a un tercero sin el conocimiento o consentimiento del usuario. [102]

5.1.4. Amenazas Emergentes en Criptomonedas

Son desafíos específicos que han surgido con la popularización y el crecimiento del mercado de criptomonedas y la tecnología blockchain. Estas amenazas son relativamente nuevas y están en constante evolución. A continuación, se describen algunas de las amenazas emergentes más destacadas relacionadas con las criptomonedas:

- **Ataques a Exchanges de Criptomonedas:** Los exchanges o casas de cambio de criptomonedas son blancos atractivos para los ciberdelincuentes. Los ataques pueden incluir el robo de criptomonedas de las plataformas de intercambio a través de vulnerabilidades de seguridad, ataques de phishing o

[101] ¿QUÉ ES un adware? [Anónimo]. Argentina.gob.ar [página web]. [Consultado el 22, octubre, 2023]. Disponible en Internet: <https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-un-adware#:~:text=Un%20adware%20es%20un%20tipo,a%20software%20o%20programa%20informático).>.

[102] ¿QUÉ ES el spyware? - Definición [Anónimo]. latam.kaspersky.com [página web]. [Consultado el 22, octubre, 2023]. Disponible en Internet: <https://latam.kaspersky.com/resource-center/threats/spyware>.

compromiso de cuentas de empleados, los cibercriminales buscan conseguir la mayor cantidad de dinero posible explotando las vulnerabilidades de estas.[103]

El 17 de enero de 2022, la plataforma de Exchange Crypto.com descubrió que un pequeño número de usuarios estaba realizando retiradas no autorizadas de criptomonedas de sus cuentas por un valor de aproximadamente 4800 ETH y 440 BTC, más unos 66.200 dólares en otras monedas. La respuesta por parte de la plataforma fue suspender las retiradas de cualquier "token" mientras se realizaba una tarea de investigación. Finalmente, ningún cliente de la plataforma sufrió pérdida de fondos, ya que los 483 usuarios afectados recibieron un reembolso completo. Esta brecha de seguridad se debió a que unos pocos usuarios estaban realizando transacciones que estaban siendo aprobadas sin el control de autenticación 2FA.[104]

- **Estafas de Inversión:** consisten en las prácticas engañosas usadas para convencer a la persona de que invierta dinero.[105] En criptomonedas, a menudo involucran promesas de altos rendimientos o esquemas de inversión fraudulentos. Los estafadores pueden persuadir a las personas para que inviertan sus criptomonedas en proyectos ficticios o esquemas Ponzi.

- **Ataques de Doble Gasto:** que las mismas unidades de una criptomoneda podrían gastarse dos veces, por lo que es crucial eliminar tecnológicamente

[103] ¿QUÉ SON los exchanges de bitcoin y otras criptomonedas? [Anónimo]. CriptoNoticias - Noticias de Bitcoin, Ethereum y criptomonedas [página web]. [Consultado el 23, octubre, 2023]. Disponible en Internet: <https://www.criptonoticias.com/criptopedia/que-son-exchanges-bitcoin-criptomonedas/>.

[104] ATAQUES A Exchanges de Criptomonedas - Security Art Work [Anónimo]. Security Art Work [página web]. [Consultado el 23, octubre, 2023]. Disponible en Internet: <https://www.securityartwork.es/2022/04/21/ataques-a-exchanges-de-criptomonedas/>.

[105] CÓMO IDENTIFICAR y prevenir los fraudes de inversiones [Anónimo]. Tennessee State Government - TN.gov [página web]. [Consultado el 23, octubre, 2023]. Disponible en Internet: <https://www.tn.gov/attorneygeneral/working-for-tennessee/consumer/resources/materials/investment-scams-sp.html#:~:text=Los%20fraudes%20de%20inversiones%20consisten,persona%20de%20que%20invierta%20dinero.>.

esta posibilidad.[106] Esto puede ocurrir en criptomonedas con retrasos en la confirmación de transacciones, como Bitcoin. Los atacantes aprovechan estos retrasos para gastar la misma moneda en dos transacciones diferentes.

- **Vulnerabilidades de Contratos Inteligentes:** Las criptomonedas basadas en contratos inteligentes, como Ethereum, pueden ser vulnerables a errores de programación en estos contratos. Los atacantes pueden explotar estas vulnerabilidades para robar fondos almacenados en contratos.

- **Ransomware de Criptomonedas:** Los ataques de ransomware encriptan los datos de una víctima y exigen un rescate en criptomonedas a cambio de la clave de descifrado. También deshabilitan las funciones de restauración del sistema, o eliminan o cifran las copias de seguridad en el ordenador o red de la víctima para aumentar la presión de pagar por la clave de descifrado. [107] Los atacantes han migrado a solicitar pagos en criptomonedas debido a su anonimato y facilidad de transferencia.

- **Suplantación de Identidad de Proyectos de Criptomonedas**: ocurre cuando un tercero se hace pasar por otra persona o entidad ya conocida por la víctima con el objetivo de robar información confidencial.[108] Los estafadores a menudo se hacen pasar por proyectos de criptomonedas legítimos en redes sociales o sitios web falsos para obtener donaciones o inversiones. Esta suplantación puede engañar a inversores y entusiastas.

---

[106] Â¿QUÃ© ES el doble gasto y por quÃ© supone un problema? [Anónimo]. [Consultado el 22, octubre, 2023]. Disponible en Internet: <https://www.bitpanda.com/academy/es/lecciones/que-es-el-doble-gasto-y-por-que-supone-un-problema/>.

[107] ¿QUÉ ES el ransomware? | IBM [Anónimo]. IBM in Deutschland, Österreich und der Schweiz | IBM [página web]. [Consultado el 23, octubre, 2023]. Disponible en Internet: <https://www.ibm.com/es-es/topics/ransomware#:~:text=El%20ransomware%20de%20criptomonedas%20comienza,por%20la%20clave%20de%20descifrado.>.

[108] QUÉ SON y cómo funcionan los ataques de suplantación de identidad [Anónimo]. EALDE Business School [página web]. [Consultado el 23, octubre, 2023]. Disponible en Internet: <https://www.ealde.es/ataques-de-suplantacion-de-identidad/>.

- **Ataques a Monederos (Wallets) de Criptomonedas:** Los monederos digitales son objetivos comunes para los ciberdelincuentes. Ya que son considerados como la solución de almacenamiento de criptomonedas más fiable. Un dispositivo especial que firma todas las operaciones del propietario en la cadena de bloques sin conexión parece mucho más seguro que las aplicaciones de ordenador o el almacenamiento online.[109] Los ataques pueden incluir la instalación de malware en dispositivos de usuarios para robar claves privadas o la suplantación de monederos en línea.

- **Robo de Identidad en Criptomonedas:** Los delincuentes pueden robar la identidad de personas para abrir cuentas en exchanges o realizar transacciones fraudulentas con criptomonedas en nombre de la víctima. Es la sustracción de información personal, imagen o posesiones con el fin de utilizarla para cometer otros delitos, ya sea para acceder a las cuentas de la víctima o para ocultar la verdadera identidad de los estafadores. Abarca una amplia gama de estafas y delitos diferente.[110]

[109] LOS MONEDEROS de criptomonedas físicos y digitales: ¿qué son y cómo se roban? [Anónimo]. Soluciones de ciberseguridad de Kaspersky para hogares y empresas | Kaspersky [página web]. [Consultado el 23, octubre, 2023]. Disponible en Internet: <https://www.kaspersky.es/blog/five-threats-hardware-crypto-wallets/28724/>.

[110] ROBO DE identidad [Anónimo]. SEON ES [página web]. [Consultado el 23, octubre, 2023]. Disponible en Internet: <https://seon.io/es/recursos/glosario/que-es-el-robo-de-identidad/#:~:text=El%20robo%20de%20identidad%20es,verdadera%20identidad%20de%20los%20estafadores.>.

5.1.5. Características de las amenazas

Comprender las características únicas de las amenazas emergentes en criptomonedas es fundamental para abordar los desafíos de seguridad en este campo. El anonimato, la falta de regulación uniforme y la naturaleza financiera de estas amenazas requieren enfoques específicos de seguridad y la promoción de la educación y la concienciación entre los usuarios de criptomonedas.

Cuadro 2. Características de las amenazas.

Característica	Amenazas Emergentes en Criptomonedas	Amenazas Tradicionales en Seguridad Digital
Naturaleza de la Amenaza	Lucrativas y enfocadas en activos financieros digitales.	Diversas y relacionadas con sistemas informáticos.
Tecnología Vulnerada	Explotan vulnerabilidades específicas en la tecnología blockchain.	Suelen afectar sistemas y redes informáticas.
Recuperación de Fondos	Difícil, ya que las transacciones de criptomonedas son irreversibles.	Posible en muchos casos, dependiendo de las circunstancias.
Nivel de Anonimato	Mayor debido a la naturaleza pseudónima de las criptomonedas.	Menos anónimas, ya que las actividades se pueden rastrear.
Regulación y Políticas	Menos regulación clara y variabilidad según la jurisdicción.	Regulación y leyes establecidas en la mayoría de los países.
Objetivo Principal	Robo de criptomonedas, estafas de inversión, explotación de vulnerabilidades.	Compromiso de sistemas, robo de datos, interrupción de servicios.
Comunidades y Redes Sociales	Suplantación de identidad de proyectos legítimos en línea.	Ataques de phishing y suplantación de identidad en redes sociales.
Ataques a Exchanges	Robo de criptomonedas de múltiples usuarios en exchanges.	No aplicable en el contexto de amenazas tradicionales en seguridad digital.

Vulnerabilidades en Contratos Inteligentes	Explotación de errores de programación en contratos inteligentes.	No aplicable en el contexto de amenazas tradicionales en seguridad digital.
Riesgos de Doble Gasto	Posibles en criptomonedas con retrasos en confirmaciones.	No aplicable en el contexto de amenazas tradicionales en seguridad digital.
Ransomware de Criptomonedas	Cifrado de datos con demandas de rescate en criptomonedas.	No aplicable en el contexto de amenazas tradicionales en seguridad digital.
Ataques a Monederos Digitales	Robo de claves privadas y suplantación de monederos en línea.	Suplantación de identidad y ataques a monederos digitales tradicionales.

Fuente: Elaboración propia con base en información de páginas web de internet: [111], [112], [113], [114], [115], [116].

[111] IBM. (s.f.). ¿Qué es la seguridad de blockchain? | IBM. IBM - United States. https://www.ibm.com/es-es/topics/blockchain-security

[112] Amenazas y Riesgos de Seguridad de Blockchain • Blog Cryptomus. (s.f.). Crypto Payment Gateway You Can Rely On. https://cryptomus.com/es/blog/4-hidden-and-rarely-discussed-security-threats-of-blockchain?srsltid=AfmBOooouveUy3eh6ikqbLatVr0fBcIWaS1llHSDTB-Zh5bgAb3KgiKtp

[113] Dolader, Bel, & Muñoz. (2023). Análisis de las amenazas económicas en la era digital. Ministerio de Turismo, Gobierno de España. Disponible en: https://www.mintur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/405/DOLADER,%20BEL%20Y%20MU%C3%91OZ.pdf

[114] Universidad Areandina. (2023). Impacto de la tecnología en el ecosistema financiero. Digitk Areandina. Disponible en: https://digitk.areandina.edu.co/server/api/core/bitstreams/dd3a40fb-196e-42b6-8e1b-4bb79d135864/content

[115] El Economista. (2018). ¿Cuáles son las principales amenazas para los usuarios de criptomonedas? Disponible en: https://www.eleconomista.com.mx/finanzaspersonales/Cuales-son-las-principales-amenazas-para-los-usuarios-de-criptomonedas-20180404-0095.html

[116] ValoraData. (2023). Criptomonedas y ciberseguridad: una creciente amenaza. Disponible en: https://www.valoradata.com/blog/criptomonedas-amenaza-ciberseguridad/

5.1.6. Comparación de amenazas

Se presenta el siguiente cuadro comparativo, el cual ofrece una visión detallada de las diferencias entre las amenazas tradicionales en seguridad digital y las amenazas emergentes relacionadas con las criptomonedas. Las amenazas emergentes representan un desafío único debido a la naturaleza descentralizada y la falta de regulación en el espacio de las criptomonedas.

Cuadro 3. Diferencias entre amenazas.

Ámbito	Amenazas Tradicionales en Seguridad Digital	Amenazas Emergentes en Criptomonedas
Naturaleza de la Amenaza	Amenazas conocidas y bien documentadas que han existido durante años.	Amenazas relativamente nuevas y en constante evolución en el contexto de las criptomonedas.
Objetivo Principal	Comprometer sistemas informáticos, robar información confidencial o interrumpir el funcionamiento normal de sistemas y redes.	Robar criptomonedas, engañar a inversores o explotar vulnerabilidades en tecnología blockchain y contratos inteligentes.
Medios de Ataque	Malware (virus, troyanos, ransomware), phishing, ingeniería social, ataques de fuerza bruta, ataques de denegación de servicio (DDoS) y otros.	Ataques a exchanges de criptomonedas, estafas de inversión, ataques de doble gasto, vulnerabilidades de contratos inteligentes y otros.
Vulnerabilidades Explotadas	Suelen explotar vulnerabilidades en sistemas, contraseñas débiles o la falta de conciencia en seguridad por parte de los usuarios.	Se basan en vulnerabilidades específicas en plataformas de intercambio, contratos inteligentes y redes de criptomonedas.
Impacto Económico	Las amenazas tradicionales pueden resultar en la pérdida de datos, la interrupción de servicios, el robo de información financiera y otros daños económicos.	Estas amenazas pueden resultar en la pérdida de criptomonedas, estafas financieras, el compromiso de contratos inteligentes y otros daños económicos relacionados con las criptomonedas.

Regulación y Políticas	Existe regulación y leyes establecidas en la mayoría de los países para abordar estas amenazas, lo que proporciona un marco legal para la protección.	La regulación en el espacio de las criptomonedas es aún incipiente en muchos lugares, lo que puede llevar a un ambiente menos regulado.
Educación y Conciencia	La educación en seguridad cibernética está ampliamente disponible y es una parte fundamental de la defensa contra estas amenazas.	La educación en seguridad de criptomonedas es una necesidad emergente y muchas personas pueden no estar bien informadas sobre los riesgos y las mejores prácticas.
Anonimato y Rastreabilidad	En general, el rastreo de actividades maliciosas puede ser más factible debido a la regulación y las herramientas de seguridad establecidas.	La naturaleza pseudónima y descentralizada de las criptomonedas puede dificultar el rastreo y la identificación de los atacantes, lo que hace que las investigaciones sean más complejas.
Tecnología Subyacente	Dependen de tecnologías tradicionales y sistemas centralizados.	Basadas en tecnología blockchain y redes descentralizadas.
Desarrollo de Soluciones de Seguridad	Soluciones de seguridad digital bien establecidas.	El desarrollo de soluciones de seguridad específicas para criptomonedas está en constante evolución.

Fuente: Elaboración propia con base en información de páginas web de internet: [117], [118], [119], [120], [121], [122], [123].

[117] Fondo Monetario Internacional (FMI) - Reporte sobre los riesgos globales de las criptomonedas y la regulación emergente: https://www.imf.org/es/Blogs/Articles/2023/01/18/crypto-contagion-underscores-why-global-regulators-must-act-fast-to-stem-risk

[118] Techopedia - Discusión sobre el impacto de las criptomonedas en la privacidad y las amenazas emergentes relacionadas: https://www.techopedia.com/es/blockchain-amenaza-privacidad-gobiernos

[119] Salazar, J. (2023). La evolución de las amenazas de ciberseguridad en las criptomonedas. Revista Digital ECOTEC. Disponible en: https://revistas.ecotec.edu.ec/index.php/rnv/article/view/604

[120] Fondo Monetario Internacional (FMI). (2023). La crisis de las criptomonedas subraya la necesidad de regulaciones globales rápidas. Disponible en: https://www.imf.org/es/Blogs/Articles/2023/01/18/crypto-contagion-underscores-why-global-regulators-must-act-fast-to-stem-risk

[121] Techopedia. (2023). Blockchain: ¿Amenaza la privacidad de los gobiernos? Disponible en: https://www.techopedia.com/es/blockchain-amenaza-privacidad-gobiernos

[122] Repositorio Digital tdea. https://dspace.tdea.edu.co/bitstream/handle/tdea/5458/Análisis_Riesgos_Amenazas_Ecosistema_Cripto_Bitcoin.pdf?sequence=1&isAllowed=y

[123] Ciberseguridad: amenanzas principales y emergentes | Temas | Parlamento Europeo. (s.f.). Temas | Parlamento Europeo.

5.1.7. Comparación Seguridad y Privacidad

La seguridad y la privacidad son pilares fundamentales en el contexto de blockchain y criptomonedas, debido que estos conceptos hacen referencia a la protección de los activos digitales y la información personal de los usuarios.

Seguridad en Criptomonedas: Se refiere a las medidas y prácticas destinadas a proteger los activos digitales, como Bitcoin, Ethereum u otras criptomonedas, contra amenazas y riesgos. Esto implica tomar medidas para proteger tanto la información sensible de los usuarios, contraseñas, como los activos digitales y las transacciones que los involucran.[124] La seguridad de las transacciones y la protección contra ataques cibernéticos en criptomonedas es esencial para evitar la pérdida de activos y garantizar la integridad de las transacciones en una red blockchain.

Privacidad en Criptomonedas: Se refiere a la protección de la información personal de los usuarios que participan en transacciones de criptomonedas. A pesar de que las transacciones en la cadena de bloques son generalmente seudónimas, es posible rastrear ciertas actividades y revelar información personal si no se toman precauciones. La privacidad en criptomonedas implica el uso de técnicas como el cifrado, la mezcla de monedas (coin mixing) y la gestión cuidadosa de datos personales para preservar la confidencialidad de los usuarios.[125]

---

https://www.europarl.europa.eu/topics/es/article/20220120STO21428/ciberseguridad-amenanzas-principales-y-emergentes

[124] SEGURIDAD DE Criptomonedas: 3 Claves Para Protegerlas - Bitso Blog [Anónimo]. Bitso Blog [página web]. [Consultado el 23, octubre, 2023]. Disponible en Internet: <https://blog.bitso.com/es-ar/seguridad-ar/seguridad-de-criptomonedas#:~:text=Implica%20tomar%20medidas%20para%20proteger,más%20popularidad%20entre%20los%20inversores.>.

[125] SEGURIDAD DE Criptomonedas: 3 Claves Para Protegerlas - Bitso Blog [Anónimo]. Bitso Blog [página web]. [Consultado el 23, octubre, 2023]. Disponible en Internet: <https://blog.bitso.com/es-ar/seguridad-ar/seguridad-de-criptomonedas#:~:text=Implica%20tomar%20medidas%20para%20proteger,más%20popularidad%20entre%20los%20inversores.>.

Por ello se entiende que la seguridad en criptomonedas se centra en la protección de los activos digitales y la infraestructura de blockchain, mientras que la privacidad en criptomonedas se enfoca en la protección de la información personal de los usuarios y en preservar su anonimato en las transacciones. Ambos aspectos son fundamentales para garantizar una experiencia segura y confidencial en el uso de criptomonedas.

6 EVALUACIÓN DE LA OPINIÓN PÚBLICA SOBRE CRIPTOMONEDAS EN COLOMBIA

Conocer la opinión pública sobre criptomonedas proporciona una guía esencial para la alineación de estrategias educativas. A medida que estas tecnologías avanzan las criptomonedas toman mayor fuerza en el panorama financiero global, por lo cual es necesario comprender los niveles de conocimiento, los mitos o teorías que puedan prevalecer en la sociedad referente a las criptomonedas. De esta manera, permite desarrollar análisis relevantes para entender la aceptación social de estas tecnologías y también desempeña un papel fundamental en la formulación de políticas, en la seguridad digital y en la educación financiera.

6.1 PUENTES DE CONOCIMIENTO: ANÁLISIS DE LA PERCEPCIÓN PÚBLICA A TRAVÉS DE ENCUESTAS

Comprender cómo el público percibe estas tecnologías es esencial para la creación de regulaciones que fomenten la innovación, protejan a los usuarios y aborden las preocupaciones legítimas. La participación del público en este proceso permite identificar y analizar la percepción sobre temas de la legalidad, seguridad, mitos comunes y servicios asociados a esta tecnología.

Esto resulta fundamental en un entorno donde las amenazas cibernéticas y los fraudes digitales pueden presentar desafíos significativos. Por tal motivo, las encuestas se consideran como herramientas valiosas para recopilar datos de manera rápida y cuantitativa, identificando percepciones comunes sobre las criptomonedas.

6.1.1. Estructura de la Encuesta

Para abordar el objetivo de entender la opinión pública sobre criptomonedas en Colombia, se diseñó una encuesta estructurada para la recolección de datos de manera cuantitativa, centrando el enfoque en obtener información detallada sobre el conocimiento actual, percepciones, mitos y actitudes de la población respecto a las criptomonedas. Esta encuesta fue enviada por medio de redes sociales como WhatsApp. A continuación, se describe el proceso de diseño, incluyendo el tipo de preguntas, la estructura adoptada:

1. **Sección Introductoria:**

Se incluyó una sección introductoria que proporcionaba contexto sobre el propósito de la encuesta, ayudando a los participantes a comprender la intención respecto del porque se aborda el tema y establecer un marco para sus respuestas.

Figura 6. Diseño de Banner e Introducción de Encuesta.

Fuente: El autor

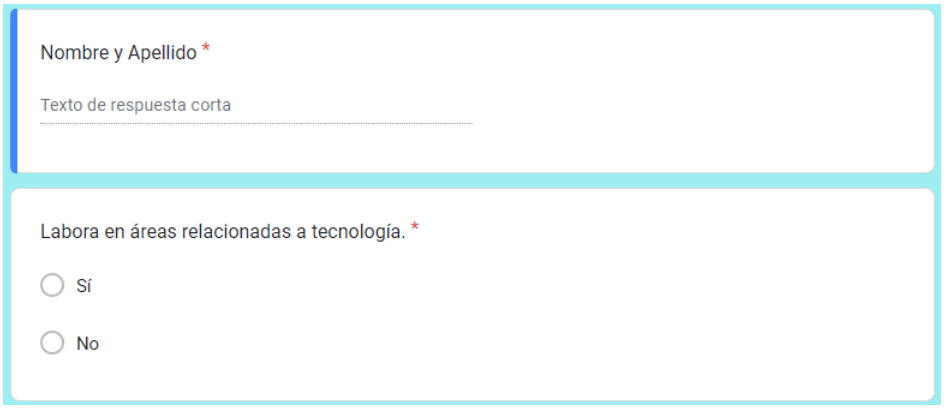
2. **Diseño de Preguntas:**

Para la encuesta, se diseñaron preguntas estructuradas para recopilar datos de los participantes, donde se incluyeron tipos de preguntas con la opción de respuesta cerradas y de opción múltiple, con la finalidad de obtener información cuantitativa sobre el nivel de conocimiento y la aceptación de las criptomonedas.

- **Sección Principal:**

La sección principal abordó preguntas relacionadas con el nombre y también se incluyó una pregunta referente al área de trabajo, esto con la finalidad de generar una ayuda para segmentar a los participantes en grupos específicos para analizar patrones o tendencias.

Figura 7. Sección Inicial Para Toma de Datos



Fuente: El autor

Preguntas Cerradas:

Posterior se incluyeron preguntas específicas sobre los niveles de conocimiento de los encuestados, las actividades en las relacionadas, legalidad, seguridad, mitos comunes y servicios asociados a esta tecnología, las preguntas diseñadas fueron las siguientes:

1. ¿Cuánto sabes sobre criptomonedas?

Marca solo un óvalo.

- Nada
- Algo
- Bastante

2. ¿Crees que las criptomonedas son legales?

Marca solo un óvalo.

- Sí
- No

3. ¿Piensas que las criptomonedas son utilizadas principalmente para actividades ilícitas?

Marca solo un óvalo.

- Sí
- No

4. ¿Consideras que las transacciones con criptomonedas son totalmente anónimas y no pueden rastrearse?

Marca solo un óvalo.

- Sí
- No

5. ¿Opinas que solo las personas con conocimientos avanzados en tecnología pueden usar criptomonedas?

Marca solo un óvalo.

- Sí
- No

6. ¿Crees que las criptomonedas son propensas a sufrir hackeos y robos?

Marca solo un óvalo.

- Sí
- No

7. ¿Opinas que las criptomonedas tienen un impacto positivo en la innovación financiera?

Marca solo un óvalo.

- Sí
- No

8. ¿Has utilizado alguna vez criptomonedas para realizar transacciones de compra o venta?

Marca solo un óvalo.

- Sí
- No

9. ¿Cuál es tu percepción sobre la seguridad de las criptomonedas?

Marca solo un óvalo.

- Muy seguras. (Sin importar los conocimientos informáticos.)
- Seguras. (Riesgosas si no se tienen conocimientos informáticos.)
- Nada seguras.

10. ¿Crees que la información sobre criptomonedas que circula en las redes sociales es confiable?

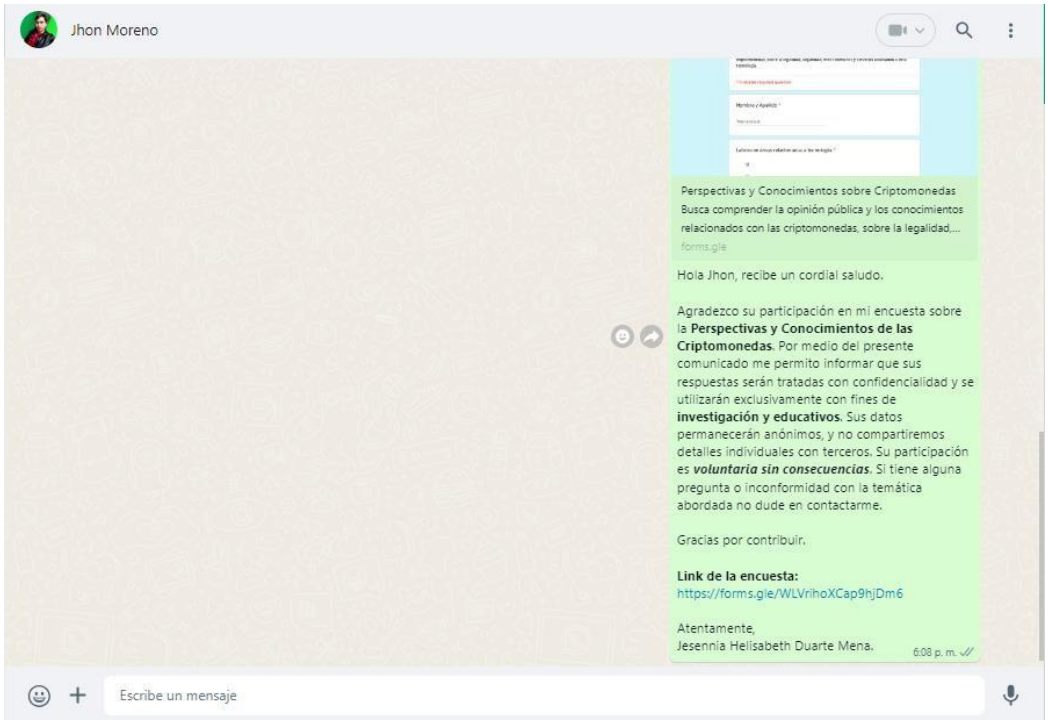
Marca solo un óvalo.

- Sí
- No

3. Pruebas Piloto

Se realizaron pruebas piloto para evaluar la claridad de las preguntas, la duración de la encuesta y la eficacia del flujo de preguntas. Los participantes fueron informados vía WhatsApp de que sus respuestas se utilizarían únicamente con fines de investigación y que no se compartirían detalles individuales.

Figura 8. Comunicado del Consentimiento Informado Para la Encuesta



Fuente: El autor

A continuación, se presenta el enlace que dirige al formulario de la encuesta estructurada para la recolección de datos.

6.1.2. Link de la Encuesta

Este hipervínculo permite a los participantes acceder al cuestionario y responder las preguntas diseñadas para explorar el conocimiento, percepciones y actitudes hacia las criptomonedas en Colombia. El enlace facilita la participación directa en el estudio, promoviendo una recopilación eficiente y accesible de información.

https://forms.gle/WLVrihoXCap9hjDm6

6.1.3. Link de Resultados de la Encuesta

El siguiente enlace permite acceder a los resultados recopilados en la encuesta sobre la opinión pública de criptomonedas en Colombia. Este hipervínculo ofrece una vista detallada a los resultados de los datos cuantitativos obtenidos.

https://drive.google.com/drive/folders/1S2D16IU2QaSlV0uqDXs3tx0LCWWhTAcp?usp=drive_link

6.1.4. Análisis de Datos Cuantitativo

Para el desarrollo de la encuesta se tomó un grupo de 50 personas, por ello, se planificó realizar un análisis cuantitativo de las respuestas, para este propósito, se utilizaron herramientas estadísticas para resumir patrones con ayuda de formularios de Google. Con este diseño de encuesta, se busca capturar una imagen completa de la opinión pública sobre criptomonedas en Colombia, proporcionando información valiosa para el desarrollo de la monografía.

6.1.5. Contextualización de Resultados

A continuación, se realiza la contextualización de los resultados obtenidos en la encuesta, ya que permite crear un puente entre los datos y así entender las respuestas obtenidas en relación con el entorno más amplio de las criptomonedas. Estas preguntas abordan una variedad de aspectos relacionados con las criptomonedas y pueden proporcionar información valiosa sobre la comprensión y las percepciones de las personas sobre este tema.

- **Nivel de conocimiento:** La primera pregunta evalúa el nivel de conocimiento de la persona sobre criptomonedas. Las respuestas pueden variar desde aquellos que tienen un conocimiento básico hasta aquellos con un entendimiento más profundo.

- **Legalidad de las criptomonedas:** La segunda pregunta busca comprender la percepción sobre la legalidad de las criptomonedas. Las respuestas pueden reflejar la comprensión de la regulación en diferentes jurisdicciones.

- **Percepción de actividades ilícitas:** La tercera pregunta explora la percepción sobre el uso de criptomonedas en actividades ilícitas. Las respuestas pueden variar y reflejar la influencia de la percepción pública y de los eventos mediáticos.

- **Anonimato de las transacciones:** La cuarta pregunta se centra en la percepción sobre el anonimato de las transacciones con criptomonedas. Las respuestas pueden abordar conceptos erróneos comunes o conocimientos precisos sobre la transparencia de la blockchain.

- **Accesibilidad tecnológica**: La quinta pregunta aborda la percepción sobre si solo las personas con conocimientos avanzados en tecnología pueden

usar criptomonedas. Las respuestas pueden revelar la percepción sobre la accesibilidad y usabilidad de las criptomonedas.

- **Seguridad de las criptomonedas:** La sexta pregunta trata sobre la percepción de la seguridad de las criptomonedas en términos de hackeos y robos. Las respuestas pueden variar desde preocupaciones fundamentadas hasta una comprensión sólida de las medidas de seguridad.

- **Impacto en la innovación financiera:** La séptima pregunta busca opiniones sobre el impacto de las criptomonedas en la innovación financiera. Las respuestas pueden reflejar percepciones sobre cómo las criptomonedas están cambiando o podrían cambiar el panorama financiero.

- **Experiencia personal:** La octava pregunta sobre si han utilizado criptomonedas para transacciones de compra o venta proporciona información sobre la experiencia práctica de las personas con las criptomonedas.

- **Percepción de seguridad**: La novena pregunta busca la percepción personal sobre la seguridad de las criptomonedas. Las respuestas pueden variar según la experiencia personal y la comprensión de las medidas de seguridad.

- **Confianza en la información:** La décima pregunta aborda la confianza en la información sobre criptomonedas que circula en las redes sociales. Las respuestas pueden indicar el grado de discernimiento y precaución al consumir información en línea.

6.1.5.1. Análisis resultados pregunta de área de trabajo.

Figura 9. Área de Trabajo.

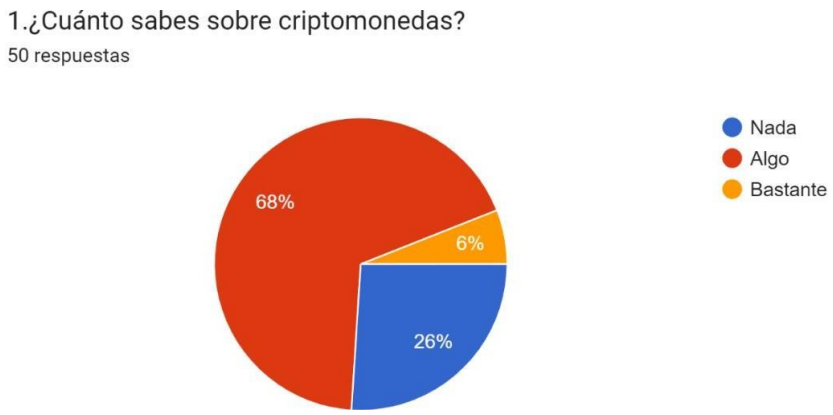
Fuente: El autor

Analizando los resultados obtenidos en la encuesta, se logra evidenciar que de las 50 personas equivalente al 100% se tiene una proporción del 62% la cual indica que trabaja en áreas de tecnología marcando una gran presencia significativa e importante. Es pregunta se planeó con la finalidad de comprender las diferencias de conocimientos o tendencias que se puedan llegar a presentar dependiendo de la población.

La pregunta se formuló con el propósito de identificar diferencias en conocimientos, habilidades y tendencias que podrían surgir en función de la ocupación de cada participante. Al comprender mejor esta distribución, se busca analizar si quienes trabajan en tecnología presentan perspectivas o competencias específicas que puedan diferenciarse de otras áreas, permitiendo así obtener insights más precisos sobre la influencia del campo laboral en los conocimientos y tendencias observadas en la encuesta.

6.1.5.2. Análisis resultados pregunta 1

Figura 10. Resultados Primera Pregunta



Fuente: El autor

Los resultados obtenidos sobre la pregunta del conocimiento de criptomonedas proporcionan información valiosa referente hacia la familiaridad que presentan las 50 personas respecto con este tema específico.

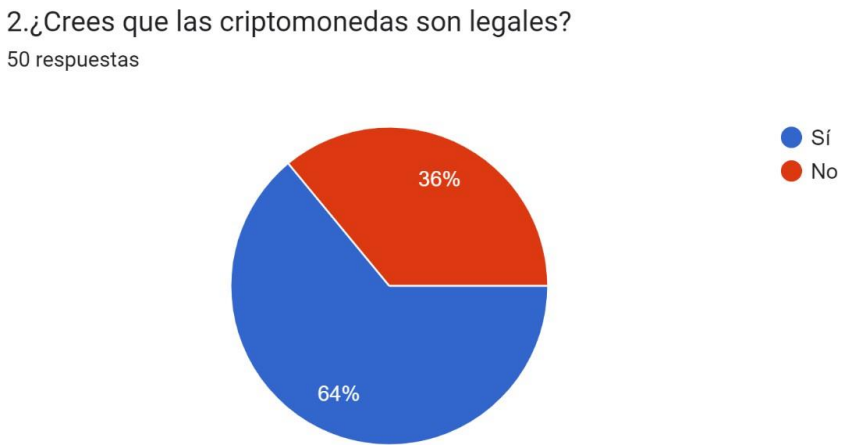
El hecho de que el 68% indique que sabe algo sobre criptomonedas sugiere que hay un nivel moderado de familiaridad dentro de la muestra. Esto podría indicar que cierta parte de las personas tienen una conciencia del concepto de criptomonedas, pero no necesariamente un conocimiento profundo y teniendo en cuenta que solo el 6% afirmó saber bastante sobre criptomonedas, podría interpretarse que existe una oportunidad para la educación y la divulgación en este tema. Por ello, el 26% que indicó no saber nada sobre criptomonedas señala una brecha en el conocimiento, esto podría ser relevante tanto para individuos como para empresas que buscan adaptarse a los cambios tecnológicos y financiero.

En conclusión, los resultados sugieren la importancia de diversificar el conocimiento en la muestra. La comprensión de las criptomonedas es cada vez más crucial en el

panorama financiero y tecnológico, hace que el bajo porcentaje de aquellos que afirman saber mucho destaca la necesidad de una mayor conciencia. Aquellos que tienen un conocimiento limitado podrían considerar la actualización de sus habilidades y conocimientos para adaptarse a un entorno que cada vez más involucra a las criptomonedas.

6.1.5.3. Análisis resultados pregunta 2

Figura 11. Resultados de Segunda Pregunta



Fuente: El autor

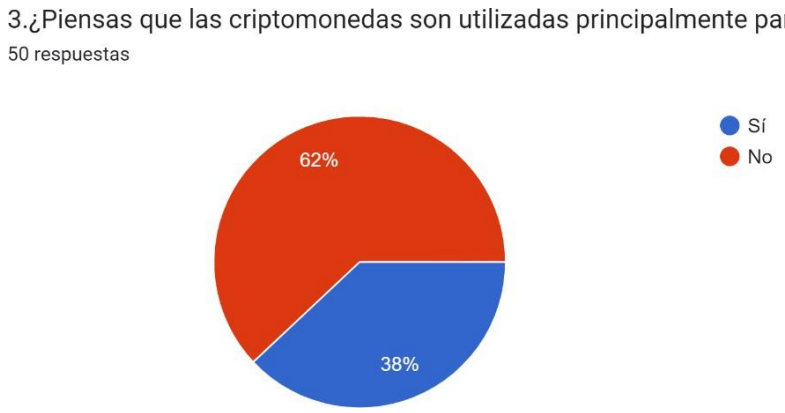
Teniendo en cuenta los resultados obtenidos, se sugiere que podría haber una oportunidad para la educación sobre las regulaciones de las monedas virtuales actualmente. Aquellos que perciben que las criptomonedas no son legales podrían beneficiarse de una comprensión más profunda de las leyes y regulaciones pertinentes, en este análisis se tiene en cuenta que el tema de las criptomonedas y su regulación están en constante evolución, por lo cual, estas opiniones podrían

cambiar con el tiempo, por el momento las percepciones sobre la legalidad de las criptomonedas pueden tener un impacto en la adopción y el uso generalizado.

Dado que el 64% de los encuestados cree que las criptomonedas son legales, esto sugiere un grado significativo de confianza en la legitimidad de estas monedas digitales y se podría reflejar una mayor aceptación y comprensión de las regulaciones en torno a las criptomonedas. Este resultado destaca la importancia de la claridad regulatoria para fomentar la adopción, ya que la educación sobre la regulación actual y los esfuerzos para establecer marcos legales pueden abordar las preocupaciones y fomentar la confianza en las criptomonedas y ser un indicativo de una mayor educación financiera y legal.

6.1.5.4. Análisis resultados pregunta 3

Figura 12. Resultados de Tercera Pregunta.



Fuente: El autor

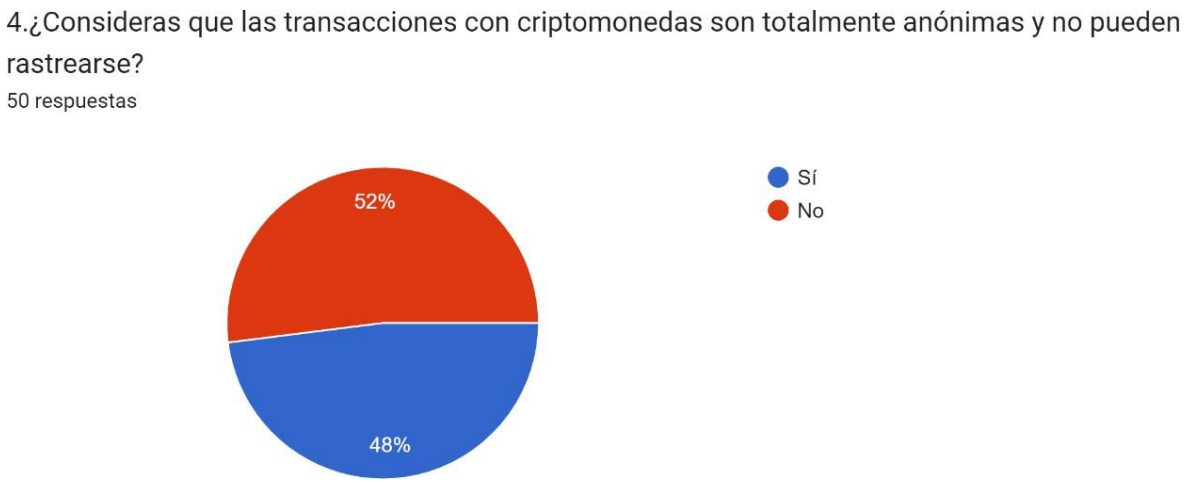
El hecho de que el 62% de las personas encuetadas crean que las criptomonedas no se utilizan principalmente para actividades ilícitas sugiere una percepción positiva, dado que no todas las criptomonedas se utilizan para actividades ilegales.

De hecho, la mayoría de las transacciones con monedas digitales son legítimas y se utilizan para diversos fines, como inversiones, transferencias de dinero, compras en línea y desarrollo de proyectos blockchain. Sin embargo, debido a la falta de regulación en algunos mercados, también se han utilizado en actividades ilegales, por ello los gobiernos y las instituciones financieras buscan abordar estos problemas y han surgido regulaciones en varios países para supervisar y controlar el uso.

Aunque la mayoría no asocia las criptomonedas con actividades ilícitas, el 38% de la muestra releja que lo cree aún, lo cual representa una proporción significativa, por lo que destaca la necesidad continua de educación para corregir percepciones erróneas y proporcionar información precisa sobre el uso legítimo de las criptomonedas.

6.1.5.5. Análisis resultados pregunta 4

Figura 13. Resultados de Cuarta Pregunta.



Fuente: El autor

Es importante destacar que ningún sistema es completamente invulnerable y las autoridades y expertos en seguridad pueden emplear diversas técnicas para rastrear actividades sospechosas en el mundo de las criptomonedas. Además, las

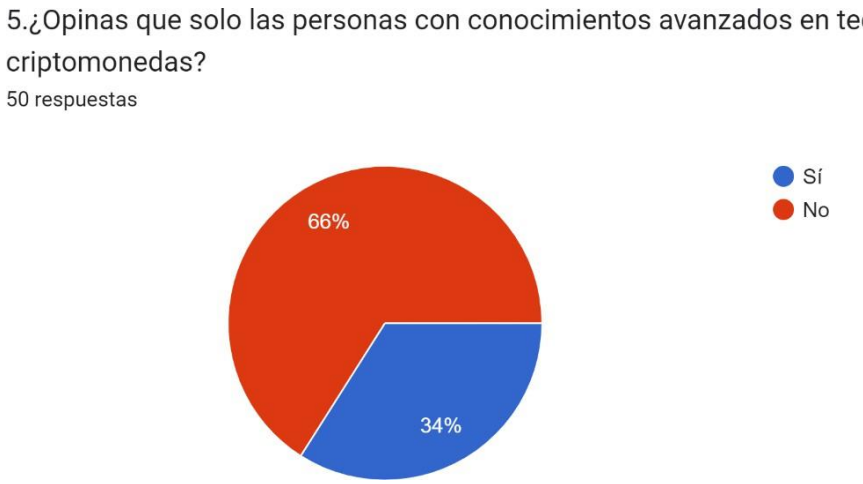
regulaciones legales pueden imponer requisitos de cumplimiento que afecten el grado de anonimato que las criptomonedas pueden ofrecer. Algunas criptomonedas, como Monero y Zcash,[126] están diseñadas específicamente para proporcionar un mayor nivel de privacidad y anonimato y utilizan técnicas avanzadas, como la mezcla de transacciones y la tecnología de prueba de conocimiento cero, para ocultar la información sobre las transacciones.

Este resultado puede indicar que los esfuerzos de desmitificación sobre la anonimidad total de las criptomonedas están teniendo impacto donde la realidad de que algunas criptomonedas ofrecen ciertos niveles de privacidad, pero no son completamente anónimas. Por ello, el hecho de que el 52% no crea que las transacciones con criptomonedas sean totalmente anónimas sugiere un nivel de conciencia sobre la trazabilidad de las transacciones, en donde se tiene una comprensión más precisa de cómo funcionan las criptomonedas. Aunque la mayoría no considera las transacciones como totalmente anónimas, el 48% que sí lo cree representa una necesidad de educación continua sobre la privacidad y la trazabilidad de las transacciones en las negociaciones con monedas digitales.

[126] MONERO, ZCASH y Dash, las mejores criptomonedas anónimas [Anónimo]. Businessinsider [página web]. [Consultado el 19, noviembre, 2023]. Disponible en Internet: <https://www.businessinsider.es/cripto/noticias/monero-zcash-dash-mejores-criptomonedas-anonimas/>.

6.1.5.6. Análisis resultados pregunta 5

Figura 14. Resultado de Quinta Pregunta.



Fuente: El autor

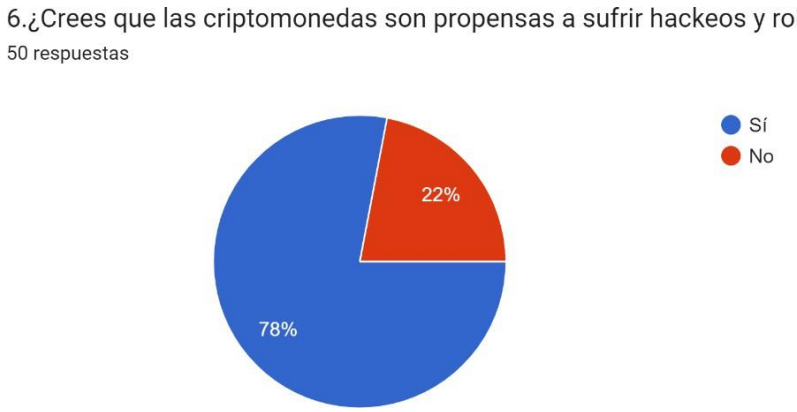
En la actualidad, existen aplicaciones y servicios que han simplificado el proceso de adquisición, almacenamiento y uso de criptomonedas, lo que facilita su acceso para un público más amplio, a menudo han sido asociadas con la tecnología y pueden requerir cierto nivel de comprensión técnica para aprovechar al máximo todas sus características, hay muchas personas que las utilizan sin ser expertos en tecnología. Las plataformas de intercambio de criptomonedas, billeteras digitales y servicios de pago han desarrollado interfaces de usuario más amigables que permiten a personas con diversos niveles de conocimientos tecnológicos participar en el mundo de las criptomonedas.

Por tal motivo es positivo que el 66% no crea que solo las personas con conocimientos avanzados en tecnología pueden usar criptomonedas en términos de accesibilidad. El 35% que piensa que se necesitan conocimientos avanzados aún señala desafíos en las percepciones, es importante abordar estas percepciones

erróneas para fomentar la adopción generalizada, que se presenta una vulnerabilidad y se deben estrategias de educación pueden personalizarse para abordar las necesidades de aquellos que aún perciben barreras tecnológicas.

6.5.1.7. Análisis resultados pregunta 6

Figura 15. Resultados de Sexta Pregunta.



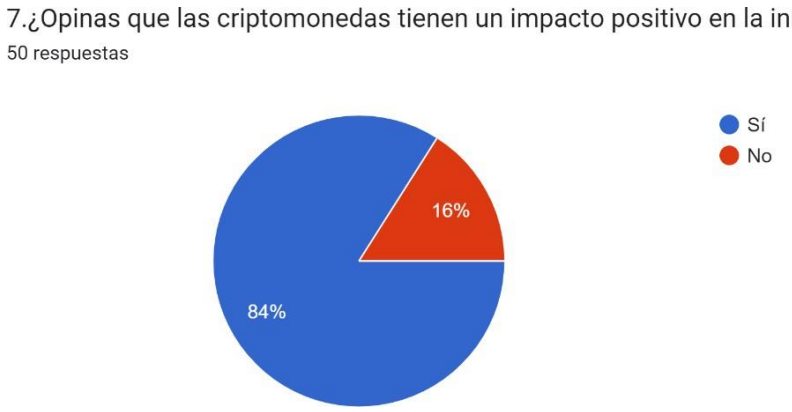
Fuente: El autor

Es importante señalar que la seguridad en el espacio de las criptomonedas ha mejorado con el tiempo en donde muchos proyectos y servicios han implementado medidas más sólidas para proteger los activos digitales y la información de los usuarios. Sin embargo, las criptomonedas han sido propensas a sufrir hackeos y robos en el pasado. La naturaleza digital y descentralizada de las criptomonedas, combinada con la irreversibilidad de muchas transacciones en la cadena de bloques, ha creado un entorno en el que los ataques pueden ser atractivos para los ciberdelincuentes. Debido que el 78% de los encuestados cree que las criptomonedas son propensas a sufrir hackeos y robos por este motivo se entiende una percepción generalizada de preocupación sobre la seguridad en el espacio de las criptomonedas y está influenciada por incidentes pasados de hackeos y robos

en intercambios de criptomonedas y otras plataformas, que han sido reportados en los medios de comunicación. Los eventos notorios en la historia de las criptomonedas, como los hackeos de intercambios, pueden haber contribuido a esta preocupación generalizada, entonces es posible que los encuestados estén más conscientes de los riesgos de seguridad en el espacio de las criptomonedas debido a la divulgación pública de incidentes de seguridad.

6.1.5.8. Análisis resultados pregunta 7

Figura 16. Resultados de Séptima Pregunta.



Fuente: El autor

Al eliminar intermediarios, como los bancos, las criptomonedas permiten transferencias de valor casi instantáneas a nivel global. Esto beneficia a las personas que envían y reciben dinero, especialmente en transacciones internacionales, al reducir costos y tiempos de espera significativamente.[127] Las

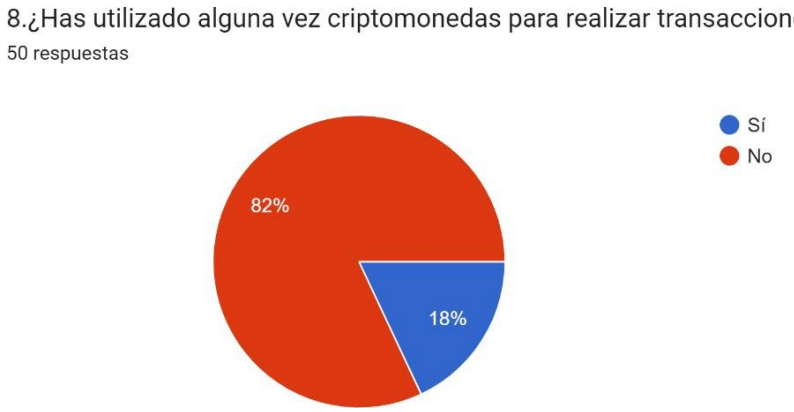
[127] CRIPTO AVANCES. EL IMPACTO DE LAS CRIPTOMONEDAS EN LA SOCIEDAD Y LA ECONOMÍA GLOBAL. LinkedIn: inicio de sesión o registro [página web]. (14, julio, 2023). [Consultado el 19, noviembre, 2023]. Disponible en Internet: <https://es.linkedin.com/pulse/el-impacto-de-las-criptomonedas-en-la-sociedad-y-economía#:~:text=Al%20eliminar%20intermediarios,%20como%20los,y%20tiempos%20de%20espera%20significativamente.>.

criptomonedas ofrecen la posibilidad de descentralizar el sistema financiero, eliminando la necesidad de intermediarios tradicionales como bancos, esto puede facilitar el acceso a servicios financieros para aquellas personas que no tienen acceso a servicios bancarios tradicionales.

Analizando las respuestas donde el 84% opina que las criptomonedas tienen un impacto positivo en la innovación financiera, sugieren una percepción generalmente favorable hacia el papel de las criptomonedas en la transformación del sector financiero y teniendo en cuenta la alta afirmación, se podría indicar la confianza en cierto punto para el papel de las criptomonedas como facilitadoras de la innovación financiera. Esto puede estar relacionado con la percepción de la tecnología blockchain como segura y confiable.

6.1.5.9. Análisis resultados pregunta 8

Figura 17. Resultados de Octava Pregunta.



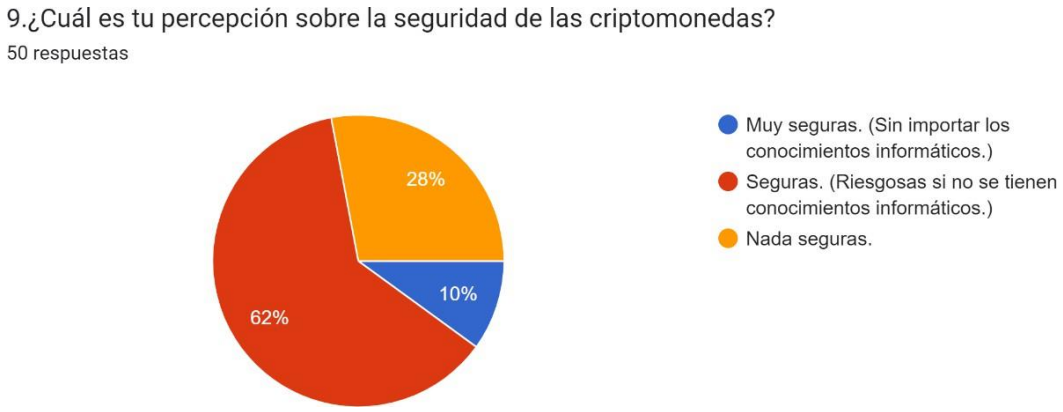
Fuente: El autor

Obtener la opinión pública sobre el uso de criptomonedas en transacciones proporciona información valiosa sobre la adopción y aceptación general de esta tecnología financiera, por este motivo conocer si las personas han utilizado

criptomonedas para comprar servicios específicos puede proporcionar información valiosa sobre los casos de uso prácticos de estas monedas digitales. El uso generalizado de criptomonedas puede contribuir a la inclusión financiera al proporcionar a las personas acceso a servicios financieros independientemente de su ubicación geográfica o situación bancaria, entonces al obtener un resultado del 82% indicando que ha utilizado criptomonedas, sugiere una adopción activa dentro de la muestra de las 50 personas indicando un creciente interés y participación en el uso de criptomonedas como medio de transacción.

6.1.5.10. Análisis resultados pregunta 9

Figura 18. Resultados de Novena Pregunta.



Fuente: El autor

La seguridad de las criptomonedas también depende en gran medida de cómo se almacenan y gestionan las claves privadas, las billeteras en línea y los exchanges pueden ser vulnerables a hackeos y el robo de claves privadas puede dar lugar a la pérdida de fondos, aunque no está directamente relacionado con la seguridad tecnológica, la volatilidad de los precios en el mercado de criptomonedas puede ser un riesgo financiero significativo para los inversores. Si bien la tecnología

subyacente de las criptomonedas proporciona un alto nivel de seguridad, la forma en que las personas gestionan sus activos digitales, la falta de regulación en algunos casos y la volatilidad del mercado pueden introducir riesgos adicionales. La educación sobre las mejores prácticas de seguridad y la comprensión de los riesgos son fundamentales para el uso seguro de las criptomonedas.

La percepción mayoritaria de que las criptomonedas son "muy seguras" refleja una confianza generalizada en la seguridad de estas tecnologías. Esto podría ser resultado de la percepción pública de que las características criptográficas y descentralizadas de las criptomonedas brindan un alto nivel de seguridad. Es posible que aquellos que han tenido experiencias positivas en el uso de criptomonedas, como transacciones y almacenamiento seguros, sean más propensos a percibirlas como muy seguras. Aunque la mayoría percibe las criptomonedas como muy seguras, el 28% que seleccionó "Nada Seguras" y el 10% que seleccionó "Nada Seguras (Sin importar los conocimientos informáticos)" indican preocupaciones significativas.

6.1.5.11. Análisis resultados pregunta 10

Figura 19. Resultados de Décima Pregunta.

Fuente: El autor

La confiabilidad de la información sobre criptomonedas que circula en las redes sociales puede variar significativamente. Las redes sociales son plataformas abiertas donde cualquier persona puede publicar contenido y esto incluye información precisa, desinformación, opiniones sesgadas y fraudes. Las redes sociales también son plataformas comunes para la promoción de estafas relacionadas con criptomonedas, por lo cual no son tan confiables y es esencial aplicar un enfoque crítico y verificar la validez de las fuentes antes de tomar decisiones basadas en esa información. La educación continua sobre las mejores prácticas en el espacio de las criptomonedas también es clave para evitar riesgos.

La alta desconfianza puede reflejar la prevalencia de desinformación, rumores o información falsa en las redes sociales sobre criptomonedas. Las plataformas de redes sociales a menudo son propensas a la difusión de noticias no verificadas o maliciosas, dejando en análisis que el bajo porcentaje de confianza en la información sobre criptomonedas en redes sociales destaca la necesidad de abordar la desinformación y mejorar la educación para construir la confianza del público en este espacio y la transparencia, la autenticidad y la promoción de fuentes confiables son elementos clave para mejorar la percepción general de la información sobre criptomonedas.

6.2 DESCUBRIMIENTOS DERIVADOS

Este estudio proporciona una visión profunda de una muestra de 50 personas sobre la opinión pública en relación con las criptomonedas, destacando áreas de entendimiento sólido y puntos de confusión. Con base en estos hallazgos, se sugiere la implementación de iniciativas educativas para abordar algunos conocimientos y aclarar mitos comunes. Además, se recomienda la colaboración con las autoridades reguladoras para mejorar la comprensión sobre la legalidad de las criptomonedas. Este capítulo ofrece una contribución valiosa al entendimiento de cómo la sociedad percibe y entiende el fenómeno de las criptomonedas.

- **Conocimiento Básico:** El análisis reveló que un porcentaje significativo de participantes tenía conocimientos básicos sobre criptomonedas, aunque existían algunas vulnerabilidades y desconocimiento en conceptos clave.

- **Legalidad:** La percepción sobre la legalidad de las criptomonedas variaba según el área de trabajo de los participantes.

- **Percepciones de Seguridad:** Hubo una división en las opiniones sobre la seguridad de las criptomonedas, con algunos participantes expresando confianza en las medidas de seguridad y otros preocupados por la susceptibilidad a hackeos.

- **Impacto en la Innovación Financiera:** La mayoría de los participantes reconocieron el potencial de las criptomonedas para impulsar la innovación financiera, aunque algunos expresaron escepticismo debido a la volatilidad del mercado.

- **Mitos Comunes y Servicios:** Las respuestas revelaron la persistencia de mitos comunes, como la asociación exclusiva de criptomonedas con

actividades ilícitas. Además, se identificaron malentendidos sobre la total anonimidad de las transacciones.

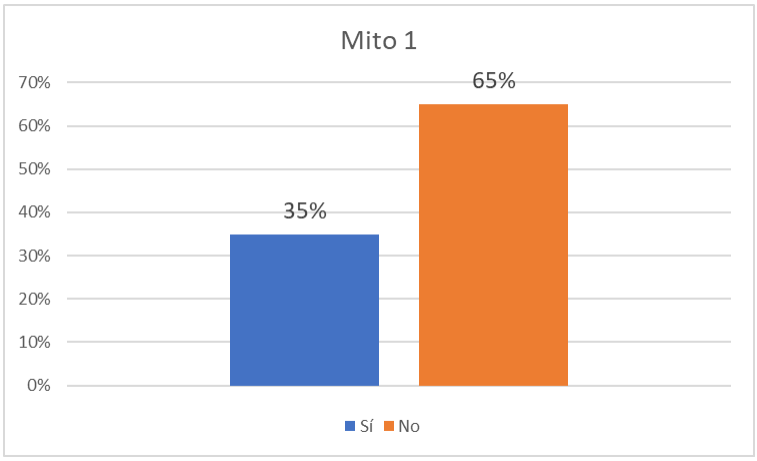
6.2.1. Identificación de Mitos Comunes

Con base en las respuestas obtenidas, se han identificado varios mitos comunes que persisten en el conocimiento popular sobre las criptomonedas. A continuación, se destacan los principales mitos revelados por los participantes:

Mito 1: Las criptomonedas son utilizadas principalmente para actividades ilícitas

Un 35% de los encuestados cree que las criptomonedas se utilizan principalmente para actividades ilícitas, lo que muestra una percepción errónea sobre el uso de estas. Si bien es cierto que las criptomonedas han sido utilizadas en algunas actividades ilegales, la mayoría de las transacciones con criptomonedas se realizan para fines legítimos, como la inversión y las compras en línea.

Figura 20. Percepción sobre el uso de criptomonedas



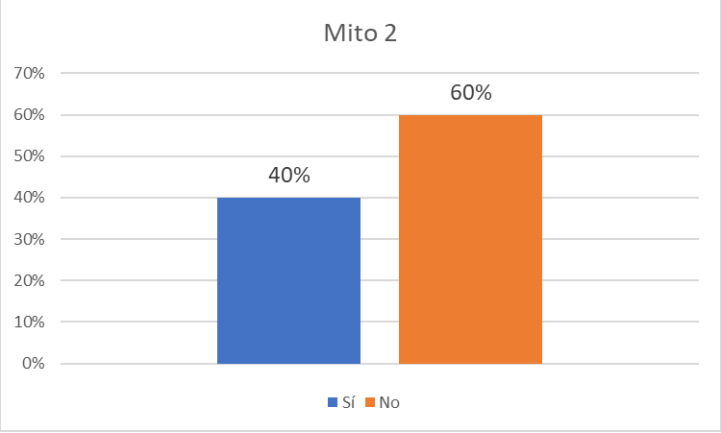
Fuente: El autor.

Sin embargo, las criptomonedas permiten realizar transacciones en cualquier parte del mundo de forma sencilla y rápida, lo que ha facilitado su uso en el comercio global. [128] Esto refleja que, aunque existen riesgos, la mayoría de las operaciones son transparentes y rastreables, lo que desmiente la creencia de que su uso principal es ilegal y permite comprender que, en realidad su adopción resalta en los mercados financieros, la tecnología y el comercio online ha superado su utilización en actividades ilícitas.

Mito 2: Solo las personas con conocimientos avanzados en tecnología pueden usar criptomonedas

El 40% de los participantes expresó que creen que solo las personas con habilidades avanzadas en tecnología pueden utilizar criptomonedas. Este mito ignora que muchas plataformas de criptomonedas y monederos digitales han simplificado el proceso, haciéndolo accesible para personas con distintos niveles de experiencia tecnológica.

Figura 21. Percepción sobre la accesibilidad de criptomonedas



Fuente: El autor.

[128] ECONOMIPEDIA. Criptomoneda. Economipedia [página web]. (25, septiembre, 2017). [Consultado el 25, septiembre, 2024]. Disponible en Internet: <https://economipedia.com/definiciones/criptomonedas.html>.

Desmentir el mito de que solo las personas con conocimientos avanzados en tecnología pueden usar criptomonedas es fundamental, ya que hoy en día, muchas plataformas han simplificado enormemente el proceso para facilitar el acceso a usuarios principiantes. Las plataformas de criptomonedas han trabajado en hacer que el proceso de compra, venta y almacenamiento de criptomonedas sea lo más sencillo posible para los principiantes.[129]

Estas plataformas, como Binance y Bitnovo, permiten a los usuarios registrarse, verificar su identidad y empezar a operar en pocos pasos, sin necesidad de tener habilidades técnicas avanzadas.[130]

Además, existen billeteras digitales que son fáciles de usar, gestionando automáticamente las claves necesarias para operar, lo que las convierte en opciones accesibles incluso para quienes no tienen experiencia previa en tecnología.[131] Esta simplificación ha permitido que personas de diversos niveles de conocimiento puedan usar criptomonedas para inversiones o transacciones cotidianas, desmintiendo así la idea de que solo los expertos pueden acceder a ellas.

[129] CRIPTOMONEDAS PARA principiantes: Guía básica para empezar [Anónimo]. Guia de Trading [página web]. [Consultado el 25, septiembre, 2024]. Disponible en Internet: <https://guiadetrading.com/criptomonedas-para-principiantes/>.
[130] CÓMO FUNCIONAN las criptomonedas: una guía para principiantes - Bitnovo Blog [Anónimo]. Bitnovo Blog [página web]. [Consultado el 25, septiembre, 2024]. Disponible en Internet: <https://blog.bitnovo.com/como-funcionan-las-criptomonedas-una-guia-para-principiantes/>.
[131] GUÍA INTRODUCTORIA de criptomonedas para principiantes [Anónimo]. BeInCrypto [página web]. [Consultado el 25, septiembre, 2024]. Disponible en Internet: <https://es.beincrypto.com/aprende/eres-nuevo-con-criptomonedas-esto-necesitas-saber/>.

Mito 3: Las transacciones con criptomonedas son totalmente anónimas y no pueden rastrearse

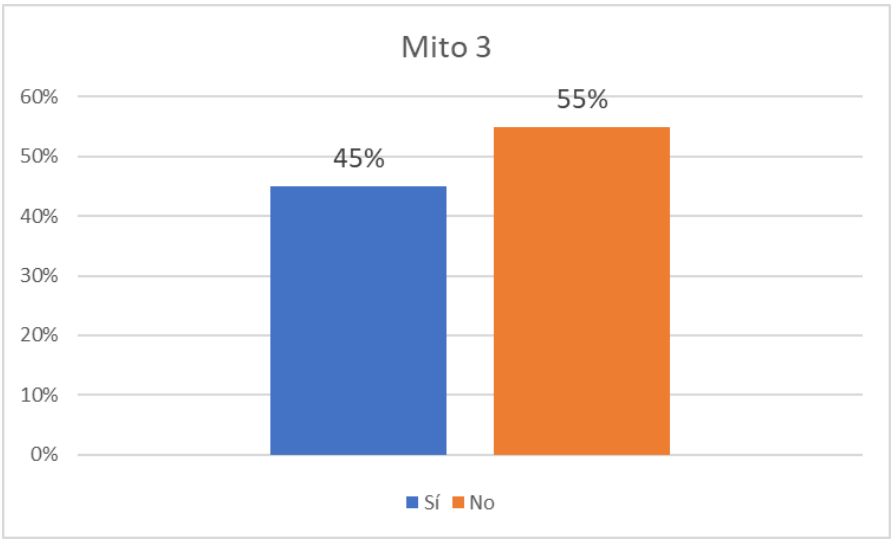
Un 45% de los encuestados considera que las transacciones con criptomonedas son completamente anónimas. Aunque las criptomonedas proporcionan cierto grado de privacidad, las transacciones realizadas en la blockchain son rastreables. Las direcciones de las billeteras no están directamente vinculadas a identidades personales, pero con suficiente investigación, es posible rastrear las transacciones.

Todas las transacciones en criptomonedas se registran en una blockchain pública, lo que permite que sean rastreables a través de herramientas de análisis de blockchain.[132] Por lo tanto, es posible vincularlas a individuos, también utilizando información adicional, como la que recopilan los intercambios de criptomonedas. Estos intercambios, por ley, deben almacenar datos de identificación de sus usuarios. Esto facilita que las autoridades gubernamentales y otros organismos rastreen las transacciones cuando sea necesario, lo que contradice la percepción de que las criptomonedas garantizan un anonimato absoluto.

Gracias al marco legal en ciberseguridad y la regulación específica en criptomonedas, es posible establecer un sistema que permite la supervisión y trazabilidad de las transacciones sin vulnerar los derechos de privacidad de los usuarios, manteniendo un equilibrio entre protección del consumidor y control sobre actividades ilícitas. De este modo, normativas como la Ley 1581 de 2012, que protege los datos personales que se mencionó anteriormente en el documento, complementa la supervisión de las actividades con criptomonedas, facilitando una transparencia regulada y acorde a la seguridad digital.

[132] ¿ES BITCOIN anónimo?: ¿Se pueden rastrear las transacciones en criptomonedas? [Anónimo]. Crypto Payment Gateway You Can Rely On [página web]. [Consultado el 25, septiembre, 2024]. Disponible en Internet: <https://cryptomus.com/es/blog/the-truth-about-anonymous-crypto-transactions>.

Figura 22. Percepción sobre el anonimato en transacciones



Fuente: El autor.

Mito 4: Las criptomonedas no están reguladas ni son legales

Aunque la mayoría de los encuestados respondió correctamente, un 30% aún cree que las criptomonedas no son legales. Si bien las criptomonedas no están reguladas en todos los países, muchos gobiernos, como el de Colombia, han comenzado a implementar marcos regulatorios o iniciativas para permitir su uso legal en ciertos contextos.

Es un error común pensar que las criptomonedas no están reguladas o que su uso es ilegal en muchos países. En Colombia, el comercio con criptoactivos no está prohibido y ya se han dado importantes pasos hacia su regulación.[133] La Superintendencia Financiera y otras entidades gubernamentales han emitido

[133] ASÍ ES La Regulación De Criptomonedas En Colombia - Bitso Blog [Anónimo]. Bitso Blog [página web]. [Consultado el 25, septiembre, 2024]. Disponible en Internet: <https://blog.bitso.com/es-co/criptomonedas-co/regulacion-criptomonedas-colombia>.

regulaciones y directrices para el manejo de criptoactivos, estableciendo controles claros para garantizar la transparencia y seguridad de las operaciones,[134] ayudando a disipar el mito de que su uso es completamente desregulado e ilegal. Normativas como la Ley 1273 de 2009 y la Ley 1581 de 2012, junto con las circulares de la Superintendencia Financiera y los lineamientos de la Superintendencia de Sociedades, no solo promueven la transparencia y la seguridad en las transacciones con criptomonedas, sino que también brindan complementos como herramientas para el monitoreo y control de actividades financieras en el ámbito digital.

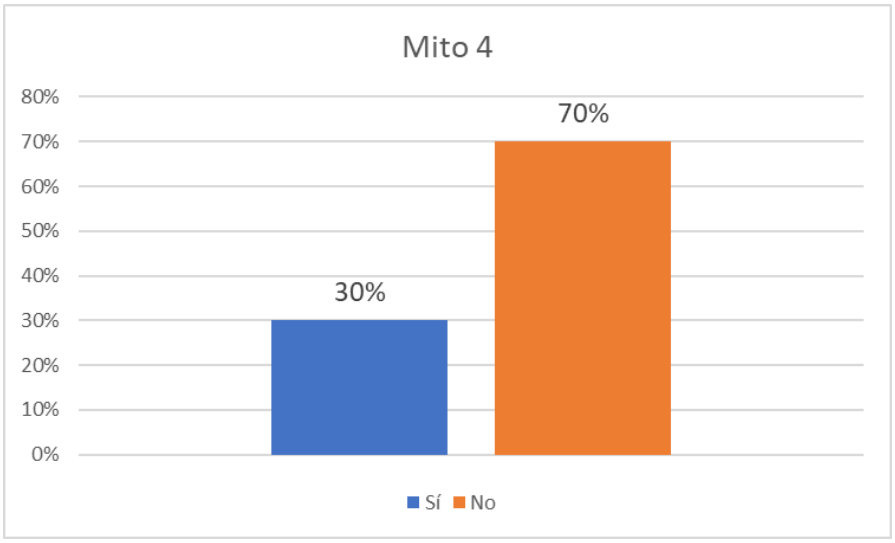
Por ejemplo, la Superintendencia de Sociedades ha implementado regulaciones que obligan a las plataformas de intercambio de criptomonedas a registrarse, cumplir con normas internacionales de contabilidad y seguridad junto con la obligación de reportar las transacciones que realizan.[135] Esto permite que las transacciones con criptomonedas sean legales en ciertos contextos, siempre que se respeten las normativas establecidas.

Es decir, que se garantiza un entorno de uso responsable y seguro de las criptomonedas, en el que tanto los usuarios como las entidades pueden contar con un marco regulatorio que promueve la innovación y la confianza en estas tecnologías dentro de parámetros de seguridad claros y efectivos.

[134] ECONOMÍA, Redacción. Criptomonedas en Colombia: ¿son legales o está incurriendo en una falta al usarlas? pulzo.com [página web]. (6, marzo, 2023). [Consultado el 25, septiembre, 2024]. Disponible en Internet: <https://www.pulzo.com/economia/criptomonedas-colombia-es-legal-como-va-su-regulacion-PP2664258A>.

[135] APROBADO PROYECTO de Ley que regula las plataformas de intercambio de criptoactivos en Colombia. [Anónimo]. Inicio | Camara de Representantes [página web]. [Consultado el 25, septiembre, 2024]. Disponible en Internet: <https://www.camara.gov.co/aprobado-proyecto-de-ley-que-regula-las-plataformas-de-intercambio-de-criptoactivos-en-colombia>.

Figura 23. Percepción sobre la legalidad de las criptomonedas



Fuente: El autor.

Como resultado estos mitos reflejan la necesidad de una mayor educación y clarificación sobre el funcionamiento y la legalidad de las criptomonedas, lo cual podría ayudar a mejorar la percepción pública y reducir el escepticismo sobre esta tecnología.

7 CATEGORIZACIÓN DE ESTRATEGIAS DE SEGURIDAD EN EL ENTORNO BLOCKCHAIN Y CRIPTOMONEDAS

El rápido crecimiento de las criptomonedas y la tecnología blockchain ha transformado el panorama financiero y digital en las últimas décadas. Lo que comenzó como una simple idea para descentralizar las transacciones financieras y eliminar intermediarios ha evolucionado hasta convertirse en una tecnología con aplicaciones que va más allá del ámbito financiero. Sin embargo, con la expansión de esta tecnología, también han surgido nuevos desafíos relacionados con la seguridad, por lo cual este capítulo busca analizar y categorizar las estrategias más populares que se utilizan en la actualidad para proteger el entorno blockchain y de criptomonedas y en donde se explorarán diversas técnicas que han sido diseñadas específicamente para abordar las amenazas emergentes en este espacio, tales como ataques a exchanges de criptomonedas, el fraude financiero y las estafas relacionadas con criptomonedas. Además, se considerarán las mejores prácticas normativas, que incluyen aspectos fundamentales para garantizar la seguridad en un entorno digital.

7.1 LA CRECIENTE RELEVANCIA DE LA SEGURIDAD EN BLOCKCHAIN

El blockchain se caracteriza por su estructura descentralizada y su capacidad de mantener registros inmutables de las transacciones.[136] Es decir, que, a diferencia de los demás sistemas tradicionales que se conocen, estos dependen de una entidad principalmente que son centralizada, por ello en las redes blockchain se distribuyen el control entre todos los nodos participantes y hace que, en teoría, sea

[136] ¿QUÉ ES la descentralización? - Explicación de la descentralización en la cadena de bloques - AWS [Anónimo]. Amazon Web Services, Inc. [página web]. [Consultado el 12, septiembre, 2024]. Disponible en Internet: <https://aws.amazon.com/es/blockchain/decentralization-in-blockchain/>.

más difícil para un solo actor llegar al punto de alterar la información registrada sin el consenso de la mayoría. No obstante, esta descentralización no está exenta de riesgo, por lo que la mayor vulnerabilidad radica en la interfaz entre los usuarios y la red blockchain, donde se encuentran los atacantes que suelen aprovechar en su gran mayoría de situaciones, la falta de medidas de seguridad adecuadas para robar activos o manipular transacciones.

Es importante categorizar las estrategias de seguridad más populares en el entorno de blockchain y criptomonedas porque esta clasificación permite entender mejor, cómo cada enfoque aborda diferentes tipos de amenazas y vulnerabilidades en este ecosistema y logra organizar las estrategias por su función y efectividad, por lo que es posible identificar cuáles son más adecuadas para mitigar riesgos específicos, para ello, se resaltan las siguientes categorías generales:

7.1.1. Categorización de Estrategias de Seguridad

La categorización de estrategias de seguridad es un proceso que organiza y clasifica las diferentes medidas que se implementan para proteger un sistema o tecnología, como el blockchain y las criptomonedas, frente a diversas amenazas. Esta clasificación ayuda a identificar amenazas potenciales y a clasificarlas según su impacto y probabilidad. Esto permite priorizar los riesgos más críticos y asignar recursos de manera efectiva,[137] abarcando tanto como ataques cibernéticos, o normativo, como el cumplimiento de leyes y regulaciones.

Es importante porque facilita una visión clara y estructurada de cómo proteger activos digitales, permitiendo a las organizaciones junto con usuarios fortalecer sus defensas ante riesgos emergentes y mejorar su capacidad de respuesta ante

[137] Acosta, D. E. (s.f.). Categorización funcional de los diferentes tipos de controles de seguridad y su aplicabilidad en la estrategia de protección corporativa. Recuperado de https://www.deacosta.com/controles-seguridad:contentReference[oaicite:0]{index=0}.

incidentes. Las estrategias de seguridad incluyen medidas preventivas, como firewalls y autenticación, que buscan evitar que los incidentes ocurran en primer lugar. También pueden incluir controles tradicionales, como cámaras de vigilancia, para desalentar intentos de ataque.[138] Para categorizar las estrategias más populares de seguridad en el entorno de blockchain y criptomonedas, se puede dividir en dos grandes grupos: estrategias técnicas y estrategias normativas y de mejores prácticas

7.1.1.1. Estrategias Técnicas

En el sector financiero, es fundamental tener una clasificación bien definida de las estrategias de seguridad para proteger la información de los clientes, garantizar la seguridad de las transacciones y cumplir con las normativas vigentes. Esto no solo aumenta la confianza de los usuarios, sino que también reduce el riesgo de fraudes y ataques cibernéticos, por ello, una adecuada implementación de estas estrategias permite la integración de nuevas tecnologías financieras de forma segura y conforme a las regulaciones establecidas.

Es importante compreneder que las estrategias técnicas se refieren a un conjunto de medidas y soluciones basadas en la tecnología para proteger sistemas, datos y redes de posibles amenazas o ataques cibernéticos.[139] Las siguientes estrategias mencionadas, están enfocadas en la infraestructura y las herramientas tecnológicas implementadas en las plataformas de blockchain para asegurar su operación y prevenir ataques.

---

[138] Microsoft. (s.f.). Definición de una estrategia de seguridad - Cloud Adoption Framework. Recuperado de https://learn.microsoft.com/es-es/cloud-adoption-framework/strategy/security:contentReference[oaicite:1]{index=1}.

[139] Diferencia entre técnica y estrategia ejemplos | Euroinnova. (s.f.). Euroinnova International Online Education.https://www.euroinnova.com/blog/diferencia-entre-tecnica-y-estrategia-ejemplos#:~:text=Son%20las%20que%20permiten%20identificar,durante%20el%20proceso%20enseñanza-aprendizaje.

- **Criptografía avanzada:** se basa en algoritmos matemáticos complejos que convierten los datos normales en una forma ilegible e ilegible para personas no autorizadas. El cifrado se utiliza para transformar el mensaje original en uno que solo puede ser leído por el destinatario autorizado, mientras que el descifrado se utiliza para convertir el texto cifrado de vuelta al texto normal.[140] Uso de algoritmos de cifrado como AES, RSA y SHA-256 aseguran la integridad y confidencialidad de los datos.

- **Contratos inteligentes auditados:** Auditorías de código para garantizar que los contratos inteligentes estén libres de vulnerabilidades. Estos son un pilar fundamental en la amplia gama de aplicaciones descentralizadas. Sin embargo, con grandes sumas de valor intercambiadas o almacenadas en ellos, se convierten en blancos lucrativos para los ciberdelincuentes.[141]

- **Pruebas de penetración (pentesting):** involucra un proceso en donde se realizan distintos tipos de tareas que identifican, en una infraestructura objetivo, las vulnerabilidades que podrían explotarse y los daños que podría causar un atacante. En otras palabras, se realiza un proceso de hacking ético para identificar qué incidentes podrían ocurrir antes de que sucedan y, posteriormente, reparar o mejorar el sistema, de tal forma que se eviten estos ataques.[142]

---

[140] Diplomado en Criptografía Avanzada. (s.f.). TECH Universidad Tecnol�gica Colombia. https://www.techtitute.com/co/informatica/diplomado/criptografia-avanzada#:~:text=La%20criptografía%20avanzada%20es%20un,avanzadas%20de%20cifrado%20y%20descifrado.

[141] ¿Qué es una auditoría de seguridad de contrato inteligente? (s.f.). BITLAB WORLD. https://bitlab.world/que-es-una-auditoria-de-seguridad-de-contrato-inteligente/#:~:text=La%20auditoría%20de%20contratos%20inteligentes,manual%20y%20pruebas%20de%20pentest.

[142] PRUEBAS DE penetración para principiantes: 5 herramientas para empezar | Revista .Seguridad [Anónimo]. Revista .Seguridad | [página web]. [Consultado el 20, septiembre, 2024]. Disponible en Internet: <https://revista.seguridad.unam.mx/numero-18/pruebas-de-penetracion-para-principiantes-5-herramientas-para-empezar>.

- **Sistemas de autenticación multifactor (MFA):** es una credencial de seguridad que verifica la identidad de un usuario cuando intenta acceder a un recurso concreto. Por ejemplo, cuando alguien inicia sesión en una cuenta de correo electrónico, suele introducir un nombre de usuario y una contraseña. Estas credenciales son una forma de identificación que indica que la solicitud de acceso procede de una persona legítima y no de un impostor.[143] Por lo cual, el agregar una capa adicional de seguridad para proteger los accesos a wallets o plataformas de criptomonedas convierte esta técnica en una de las más populares.

- **Redes descentralizadas con alta redundancia:** Asegurar que la red blockchain esté suficientemente descentralizada para prevenir ataques del 51%, de Sybil, DDoS y la manipulación de la cadena de bloques. La redundancia es en pocas palabras un respaldo, de aquellos datos o hardware de carácter crítico que se quiere asegurar ante la posibilidad de fallos que pudieran surgir debido al desgaste natural del uso ya sea del hardware o software. Se presenta como una solución a los problemas de protección y confiabilidad.[144]

- **Mecanismos de consenso seguros:** Implementación de mecanismos como Prueba de Participación (PoS) o Prueba de Trabajo (PoW) que garantizan la seguridad de la red y hacen que los ataques sean costosos y poco factibles.[145]

---

[143] ENTRUST. ¿Qué es la MFA? entrust [página web]. [Consultado el 23, septiembre, 2024]. Disponible en Internet: <https://www.entrust.com/es/resources/learn/what-is-multi-factor-authentication-mfa>.

[144] TELECOM, C3NTRO. ¿Qué es la alta disponibilidad y redundancia en la nube? C3ntro Telecom Proveedor de Servicios de Telecomunicaciones [página web]. (30, septiembre, 2021). [Consultado el 25, septiembre, 2024]. Disponible en Internet: <https://www.c3ntro.com/es-mx/blog/que-es-alta-disponibilidad-y-redundancia-en-conectividad-a-la-nube>.

[145] arXiv.org e-Print archive [página web]. [Consultado el 25, septiembre, 2024]. Disponible en Internet: <https://arxiv.org/pdf/1710.09437.pdf>.

- **Protección de claves privadas**: La custodia segura de claves privadas es esencial para evitar robos de criptomonedas. Estrategias como las billeteras hardware o multifirma (multisig) aumentan la seguridad.[146]

En la siguiente imagen anexada, se logra evidenciar la interacción entre las diferentes estrategias técnicas de seguridad en el entorno de blockchain, facilitando la comprensión de cómo cada estrategia contribuye a proteger la red, sino que también destaca el enfoque integral necesario para mitigar las amenazas emergentes.

Figura 24. Interacción de las estrategias técnicas

Fuente: El autor.

[146] SOK: RESEARCH Perspectives and Challenges for Bitcoin and Cryptocurrencies [Anónimo]. IEEE Xplore [página web]. [Consultado el 23, septiembre, 2024]. Disponible en Internet: <https://ieeexplore.ieee.org/document/7163021>.

Al mapear visualmente los mecanismos de seguridad, se obtiene una visión clara de cómo estas soluciones se interconectan para garantizar la seguridad de la red y la integridad de las transacciones. En Colombia, las estrategias técnicas están reguladas principalmente por la Superintendencia Financiera y la Ley de Protección de Datos Personales bajo la Ley 1581 de 2012, que exigen a las entidades financieras implementar medidas adecuadas para garantizar la seguridad de la información.

Esta regulación busca que los bancos adopten mecanismos de seguridad que permitan salvaguardar la confidencialidad, integridad y disponibilidad de la información financiera de sus clientes.[147] En el caso de los bancos, muchas instituciones en Colombia han implementado estas estrategias técnicas como parte de sus esfuerzos para mitigar el riesgo de ciberataques y proteger los activos financieros de sus clientes. Por ejemplo, el Grupo Bancolombia ha desarrollado un robusto sistema de ciberseguridad que incluye el uso de inteligencia artificial para detectar amenazas en tiempo real, así como la autenticación biométrica para validar las transacciones.[148] Otros bancos como Davivienda y BBVA también han implementado tecnologías avanzadas como el uso de cifrado y MFA para asegurar la seguridad de sus plataformas y proteger los datos de sus usuarios.

[147] Superintendencia Financiera de Colombia. (2021). Normativa de seguridad informática y protección de datos. Recuperado de https://www.superfinanciera.gov.co/jsp/index.jsp

[148] BANCOLOMBIA: PROMOVEMOS desarrollo económico sostenible. ¡Conoce más! [Anónimo]. Grupo Bancolombia [página web]. [Consultado el 24, septiembre, 2024]. Disponible en Internet: <https://www.grupobancolombia.com/wps/portal/acerca-de/ciberseguridad-en-bancolombia>.

7.1.1.2. Estrategias Normativas y de Mejores Prácticas

Con la necesidad de proteger a los usuarios e inversores de las crecientes amenazas en el mundo de las criptomonedas, tales como fraudes, lavado de dinero y robo de activos, la falta de regulación y el anonimato que muchas veces caracterizan a las transacciones en blockchain pueden ser explotados por actores malintencionados, por lo que es esencial contar con un conjunto de normativas claras y mejores prácticas que fomenten la protección y el buen uso de esta tecnología. A continuación, se enlistan las mejores prácticas adoptadas por las plataformas y exchanges, tales como:

- **Cumplimiento de la Ley de Habeas Data (Ley 1581 de 2012):** Esta ley regula la protección de datos personales en Colombia. Reconoce y protege el derecho que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos que sean susceptibles de tratamiento por entidades de naturaleza pública o privada.[149] Las entidades bancarias deben garantizar que la información personal de sus clientes sea tratada con confidencialidad y que los datos estén protegidos contra accesos no autorizados.

- **Conoce a tu Cliente (KYC):** Es la práctica que realizan las compañías para verificar la identidad de sus clientes cumpliendo con las exigencias legales y las normativas y regulaciones vigentes, tales como AML, LGPD y el DAS. [150] Este proceso es obligatorio para todas las entidades financieras, donde

[149] POLÍTICA DE Protección de Datos Personales - [Anónimo]. Inicio - Bienvenido al Ministerio de Ambiente y Desarrollo Sostenible - [página web]. [Consultado el 23, septiembre, 2024]. Disponible en Internet: <https://www.minambiente.gov.co/politica-de-proteccion-de-datos-personales/#:~:text=Ley%20de%20Protección%20de%20Datos,de%20naturaleza%20pública%20o%20privada.>.

[150] KYC (KNOW Your Customer): qué es y su actualidad en 2024 [Anónimo]. Signicat [página web]. [Consultado el 24, septiembre, 2024]. Disponible en Internet: <https://www.signicat.com/es/blog/kyc-know-your-customer#:~:text=¿Qué%20significa%20KYC?,como%20AML,%20LGPD%20y%20eIDAS.>.

deben recopilar y verificar la información de identidad de los clientes, dado que este control se implementa para evitar el lavado de activos y la financiación del terrorismo.

- **Normativa SARLAFT (Sistema de Administración del Riesgo de Lavado de Activos y Financiación del Terrorismo):** Es el mecanismo que permite a las entidades prevenir la pérdida o daño que pueden sufrir por su propensión a ser utilizadas como instrumento para el lavado de activos y/o canalización de recursos hacia la realización de actividades terroristas, por sus clientes o usuarios.[151] Las entidades bancarias están obligadas a implementar sistemas para la detección y reporte de actividades sospechosas relacionadas con este tipo de actividades ilegales o la financiación del terrorismo.

- **Basilea III:** Se han formulado para ser aplicados entre 2013 y 2019 como parte de un proyecto de convergencia gradual adelantado por el Gobierno Nacional, que busca promover la resiliencia del sistema financiero frente a choques adversos y apuntar a lograr la expansión y consolidación entre mercados de diversas jurisdicciones.[152] Entonces, las entidades bancarias en Bogotá deben adherirse a las directrices de Basilea III para mantener una adecuada capitalización y gestión de riesgos. Esto incluye mantener niveles mínimos de capital y fortalecer la gestión de riesgos operacionales y de mercado.

---

[151] SARLAFT [Anónimo]. Supervigilancia [página web]. [Consultado el 21, septiembre, 2024]. Disponible en Internet: <https://www.supervigilancia.gov.co/sarlaft/publicaciones/10005/sarlaft/#:~:text=32.,propensión%20a%20ser%20utilizadas%20(…)>.

[152] ESTÁNDARES DE Basilea Audit BDO Colombia [Anónimo]. BDO en Colombia - Inicio | Personas ayudando a personas a alcanzar sus sueños - BDO [página web]. [Consultado el 21, septiembre, 2024]. Disponible en Internet: <https://www.bdo.com.co/es-co/publicaciones/boletines-audit/estado-actual-del-proceso-de-convergencia-a-los-estandares-de-basilea-iii#:~:text=En%20Colombia,%20los%20principios%20de,la%20expansión%20y%20consolidación%20entre>.

- **ISO/IEC 27001:2013 (Sistema de Gestión de la Seguridad de la Información - SGSI):** Este sistema se utiliza para proteger la confidencialidad, integridad y disponibilidad de la información. La norma proporciona un marco para la seguridad de la información que ayuda a las organizaciones a identificar y gestionar sus riesgos de seguridad de la información de manera efectiva.[153] En las entidades financieras de Colombia, la implementación de esta norma asegura que las instituciones mantengan los datos financieros seguros y gestionen eficazmente los riesgos de ciberseguridad. Esto es clave para prevenir fraudes y proteger la información sensible de los clientes.

- **ISO/IEC 27005:2018 (Gestión del Riesgo de Seguridad de la Información):** Este sistema se utiliza para proteger la confidencialidad, integridad y disponibilidad de la información. La norma proporciona un marco para la seguridad de la información que ayuda a las organizaciones a identificar y gestionar sus riesgos de seguridad de la información de manera efectiva.[154] Permite a las entidades bancarias gestionar los riesgos de manera proactiva, evaluando continuamente las amenazas emergentes como los ciberataques y ajustando sus medidas de seguridad en consecuencia.

- **ISO 22301:2019 (Gestión de la Continuidad del Negocio):** Es la norma internacional para la Gestión de la Continuidad de Negocio (SGCN). Para ello, la norma proporciona un marco práctico con el fin de establecer y

[153] ¿QUÉ ES la norma ISO 27001 y para qué sirve? [Anónimo]. GlobalSuite Solutions [página web]. [Consultado el 23, septiembre, 2024]. Disponible en Internet: <https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-27001-y-para-que-sirve/#:~:text=La%20norma%20ISO%2027001%20es,y%20disponibilidad%20de%20la%20información.>.

[154] GlobalSuite Solutions [página web]. [Consultado el 24, septiembre, 2024]. Disponible en Internet: <https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-27001-y-para-que-sirve/#:~:text=La%20norma%20ISO%2027001%20es,y%20disponibilidad%20de%20la%20información.>.

gestionar un sistema de gestión de continuidad de negocio eficaz.[155] En el sector bancario, esta norma es fundamental para asegurar la continuidad de los servicios financieros en situaciones de emergencia, desastres naturales o ataques cibernéticos. Esto incluye mantener la operatividad de los sistemas críticos como las plataformas de pagos.

- **COBIT 2019:** Emerge como una herramienta crucial para las organizaciones que buscan optimizar sus procesos de tecnología de la información, debido que proporciona un enfoque integral para la gestión y gobierno de las tecnologías de la información. [156]

  COBIT se utiliza para garantizar que la tecnología y la información se gestionen de manera efectiva y que estén alineadas con los objetivos regulatorios y de negocio. Esto incluye:

  - ✓ Control y mitigación de riesgos por que proporciona un marco para identificar y mitigar riesgos tecnológicos y operacionales.
  - ✓ Mejora de la seguridad de la información mediante controles específicos, COBIT permite establecer y mantener prácticas de seguridad para proteger los activos digitales de la organización.

[155] NQA CERTIFICATION Body [Anónimo]. NQA Global Accredited Certification Body [página web]. [Consultado el 23, septiembre, 2024]. Disponible en Internet: <https://www.nqa.com/es-co/certification/standards/iso-22301#:~:text=La%20ISO%2022301%20es%20la,y%20recuperarse%20de%20incidentes%20inesperados.>.

[156] NQA Global Accredited Certification Body [página web]. [Consultado el 23, septiembre, 2024]. Disponible en Internet: <https://www.nqa.com/es-co/certification/standards/iso-22301#:~:text=La%20ISO%2022301%20es%20la,y%20recuperarse%20de%20incidentes%20inesperados.>.

- ✓ COBIT ayuda a las entidades financieras a cumplir con las regulaciones locales e internacionales relacionadas con la gestión de TI y la seguridad de la información.[157]

- **PCI DSS (Payment Card Industry Data Security Standard):** Es un foro mundial abierto destinado a la formulación, la mejora, el almacenamiento, la difusión y la aplicación permanentes de las normas de seguridad para la protección de datos de cuentas.[158] Las entidades financieras que procesan pagos con tarjetas de crédito deben cumplir con estos estándares para proteger la información del titular de la tarjeta contra el robo y el fraude. Esto implica implementar medidas como la encriptación de datos, controles de acceso y auditorías regulares.

7.2 EFECTIVIDAD DE LAS ESTRATEGIAS

La efectividad de las estrategias normativas y de mejores prácticas se ha convertido en un elemento crítico para asegurar la estabilidad, la seguridad y el cumplimiento normativo. En el sector financiero de Bogotá, estas estrategias no solo están diseñadas para mitigar riesgos emergentes como los ciberataques, sino también para cumplir con las estrictas regulaciones impuestas por entidades regulatorias nacionales e internacionales.

[157] ¿QUÉ ES el COBIT 2019? - PMG SSI - ISO 27001 [Anónimo]. PMG SSI - ISO 27001 [página web]. [Consultado el 25, septiembre, 2024]. Disponible en Internet: <https://www.pmg-ssi.com/2023/12/que-es-el-cobit-2019/>.

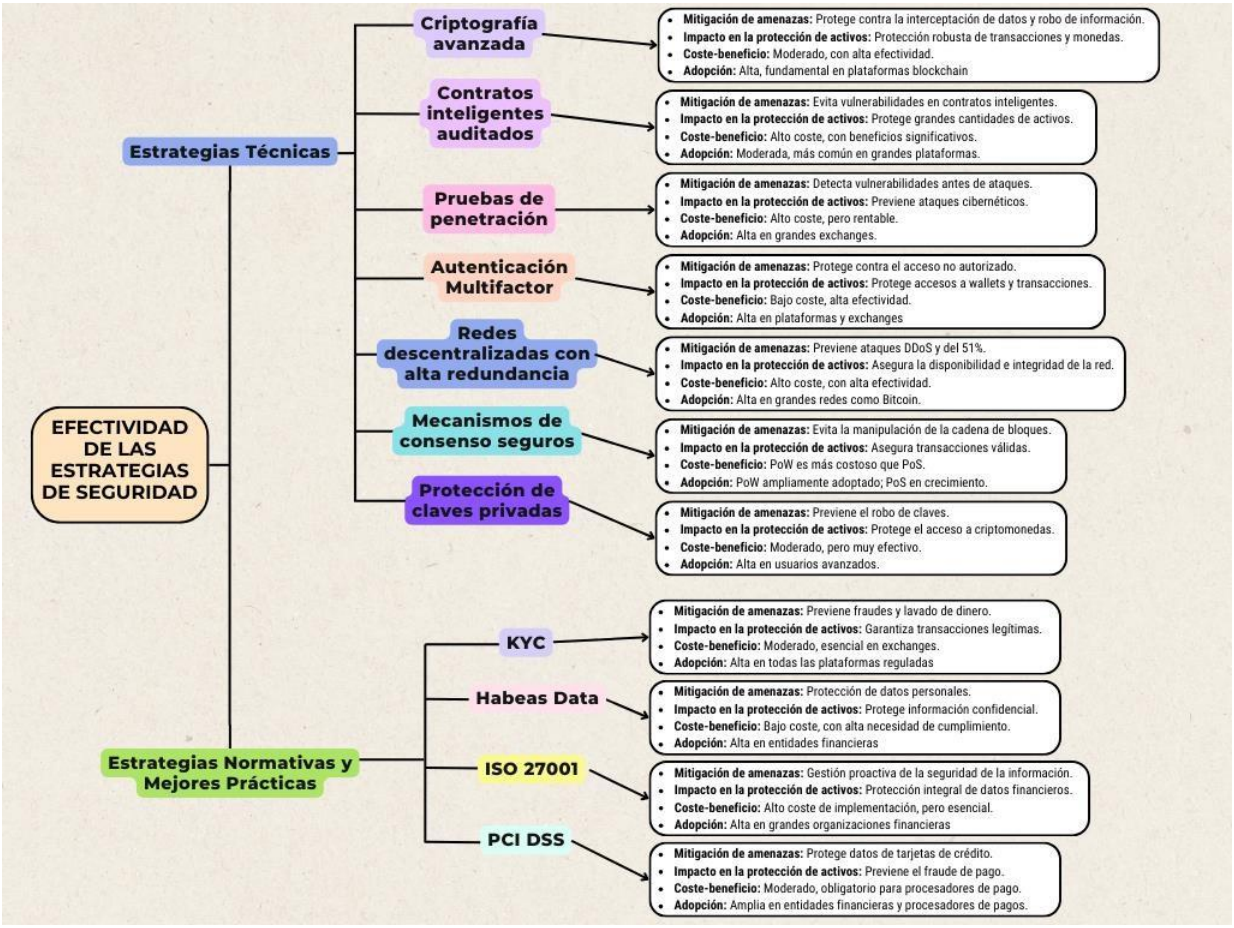
[158] SITIO OFICIAL del Consejo sobre Normas de Seguridad de la PCI (Industria de tarjetas de pago) - Verificar las normas de Cumplimiento, de seguridad de descarga de datos y de seguridad de tarjetas de crédito [Anónimo]. Not Used - Minisite [página web]. [Consultado el 25, septiembre, 2024]. Disponible en Internet: <https://www.pcisecuritystandards.org/minisite/es-es/>.

Al comprender estos factores, se puede valorar el impacto tangible de las medidas de seguridad y control en el contexto de las entidades bancarias en Bogotá, así como su contribución al fortalecimiento del sistema financiero en su conjunto.

Link:

https://www.canva.com/design/DAGRyplQQHs/qOABNX9U4gmlcnehvJLWyg/view?utm_content=DAGRyplQQHs&utm_campaign=designshare&utm_medium=link&utm_source=editor

Figura 25. Beneficios de las estrategias



Fuente: El autor.

A continuación, se presenta una tabla que vincula ejemplos reales de estas amenazas con las estrategias de seguridad más eficaces, subrayando la importancia de la implementación de medidas proactivas para proteger los activos digitales y mantener la confianza en el ecosistema cripto, dado que, a medida que los ataques y vulnerabilidades se diversifican, las estrategias de seguridad deben evolucionar para mitigar eficazmente estos riesgos.

Cuadro 4. Ejemplo de vinculación de algunas amenazas emergentes

Amenaza	Estrategia de Seguridad	Ejemplo Real
Ataques de phishing	Autenticación multifactor (2FA), Detección avanzada de amenazas	En 2024, se perdieron casi 500 millones de dólares debido a ataques de phishing en criptomonedas, según el informe de CertiK.[159]
Ataques del 51%	Redes descentralizadas con alta distribución de poder de hash	En 2021, un ataque del 51% afectó a la red de Bitcoin SV, explotando su estructura para manipular transacciones.[160]
Robo de criptomonedas en exchanges	Uso de monederos fríos y autenticación multifactor	El ataque a Binance en 2022 resultó en el robo de 570 millones de dólares al aprovechar un puente entre cadenas vulnerables.[161]
Vulnerabilidades en contratos inteligentes	Auditorías de seguridad y contratos inteligentes seguros	En 2021, los atacantes aprovecharon una vulnerabilidad en

[159] CRIPTOBALLENA PIERDE USD 55 millones de DAI en ataque de phishing [Anónimo]. Cointelegraph [página web]. [Consultado el 25, septiembre, 2024]. Disponible en Internet: <https://es.cointelegraph.com/news/crypto-whale-loses-55m-phishing-attack>.
[160] LOS 8 ataques al intercambio de criptomonedas que debes conocer [Anónimo]. Kaspersky [página web]. [Consultado el 25, septiembre, 2024]. Disponible en Internet: <https://www.kaspersky.es/resource-center/threats/crypto-exchange-hacks>.
[161] LOS 8 ataques al intercambio de criptomonedas que debes conocer [Anónimo]. Kaspersky [página web]. [Consultado el 25, septiembre, 2024]. Disponible en Internet: <https://www.kaspersky.es/resource-center/threats/crypto-exchange-hacks>.

		Poly Network, robando 611 millones de dólares de la plataforma.[162]
Ransomware exigiendo criptomonedas	Copias de seguridad, cifrado y detección de malware	Los ataques de ransomware piden pagos en criptomonedas debido al anonimato que ofrecen.[163]

Fuente: Elaboración propia con base en información de páginas web de internet.

7.3 CASOS DE ÉXITO EN LA IMPLEMENTACIÓN DE BLOCKCHAIN EN EL SECTOR FINANCIERO COLOMBIANO

En Colombia, varias empresas del sector financiero han logrado implementar estrategias de seguridad basadas en blockchain con gran éxito, considerando el enfoque financiero se puede estudiar los siguientes casos de ejemplo, como el Banco Davivienda, el cual participó en un plan piloto de emisión de bonos utilizando blockchain, lo que permitió la emisión, negociación y registro de pagos de manera completamente segura y transparente. Este proyecto, respaldado por el Banco Interamericano de Desarrollo (BID), demostró cómo la tecnología blockchain puede reducir significativamente el fraude y aumentar la confianza en los procesos financieros.[164]

Otra iniciativa exitosa es la de Credibanco, que ha utilizado la tokenización de activos para mejorar la seguridad en las transacciones digitales, permitiendo así una mayor trazabilidad y reducción de riesgos en el sector financiero. Esta adopción de blockchain ha sido clave para modernizar sus sistemas y garantizar la protección de

[162] LOS 8 ataques al intercambio de criptomonedas que debes conocer [Anónimo]. Kaspersky [página web]. [Consultado el 25, septiembre, 2024]. Disponible en Internet: <https://www.kaspersky.es/resource-center/threats/crypto-exchange-hacks>.
[163] PROTEGIENDO TUS Criptomonedas de Ataques de Phishing [Anónimo]. Bitstamp Trusted Crypto Exchange [página web]. [Consultado el 25, septiembre, 2024]. Disponible en Internet: <https://www.bitstamp.net/es/learn/security/protecting-your-crypto-from-phishing-attacks/>.
[164] SUPERFINANCIERA FINALIZA plan piloto para regular las criptomonedas en Colombia [Anónimo]. Lexir LATAM [página web]. [Consultado el 25, septiembre, 2024]. Disponible en Internet: <https://lexir.co/2022/10/24/superfinanciera-finaliza-plan-piloto-para-regular-las-criptomonedas-en-colombia/>.

los datos de los usuarios.[165] El uso de blockchain en este proceso no solo incrementa la seguridad de las transacciones digitales, sino que también ha proporcionado una trazabilidad completa de los activos tokenizados.

Lo cual permite operar con mayor eficiencia y ofrecer servicios más confiables a sus clientes. Esto es particularmente relevante en un entorno donde los consumidores exigen cada vez más seguridad y rapidez en las transacciones digitales. La implementación de estas tecnologías ha colocado a Credibanco a la vanguardia de la innovación financiera en Colombia, destacándose como un líder en el uso de soluciones basadas en blockchain para garantizar la protección de los datos y la seguridad en las transacciones.

Finalmente, el hecho de que Credibanco haya logrado reducir los riesgos inherentes al manejo de grandes volúmenes de datos financieros subraya el éxito de esta iniciativa, ya que mejora la resistencia del sistema ante ciberataques y aumenta la confianza de sus clientes y aliados comerciales.

Otro ejemplo con vinculación a nivel internacional, lo planeta la Superintendencia Financiera de Colombia, la cual ha creado un sandbox regulatorio para probar el uso de criptomonedas y blockchain con varias entidades bancarias locales. Este esfuerzo regulatorio es vital para que las instituciones financieras colombianas puedan adoptar estas tecnologías de manera segura y cumplan con las normativas globales, ayudando a mitigar el fraude y aumentar la transparencia en el uso de activos digitales.[166] Entonces, este sandbox ofrece un espacio donde las instituciones pueden probar nuevas tecnologías y modelos de negocio sin arriesgar la estabilidad financiera o la protección del consumidor, lo cual es crucial en un

[165] 35% DE empresas colombianas ya implementan blockchain, revela estudio - Soy Hodler [Anónimo]. Soy Hodler [página web]. [Consultado el 25, septiembre, 2024]. Disponible en Internet: <https://soyhodler.com/colombia-apuesta-al-crecimiento-adoptando-blockchain-y-tecnologia-web3/>.

[166] BANCOLOMBIA. Aplicaciones de la tecnología blockchain en Colombia 2022. Bancolombia [página web]. (29, junio, 2022). [Consultado el 25, septiembre, 2024]. Disponible en Internet: <https://www.bancolombia.com/empresas/capital-inteligente/tendencias/innovacion/tendencias-blockchain-2022-colombia-origen-y-aplicacion>.

sector tan delicado como el financiero. Por ello, esta iniciativa permite a los bancos y otras entidades explorar las ventajas del blockchain, como la trazabilidad, la transparencia y la reducción de fraudes, sin las presiones inmediatas del mercado, asegurando que Colombia se mantenga alineada con los estándares internacionales y permite al país incorporar criptoactivos en su sistema económico de forma confiable y efectiva.

8 CONCLUSIONES

La monografía ha destacado la importancia crítica de la seguridad en el entorno de las criptomonedas. En un mundo digital en constante evolución, donde las amenazas emergentes son una realidad, la implementación de estrategias de seguridad sólidas es esencial para proteger los activos digitales y garantizar la integridad de las transacciones en Colombia.

La comparación entre amenazas emergentes específicas del ámbito de las criptomonedas y blockchain frente a las amenazas tradicionales en seguridad digital revela que, aunque existen similitudes en las técnicas utilizadas, las amenazas emergentes representan desafíos únicos debido a la naturaleza descentralizada y transparente de la tecnología blockchain. A diferencia de los sistemas tradicionales, donde los ataques suelen dirigirse a entidades centralizadas, en blockchain los ataques pueden enfocarse en el consenso de la red o en el control de claves privadas. Esto subraya la necesidad de adaptar las estrategias de defensa y gestión de riesgos a las particularidades de las criptomonedas y blockchain, lo cual es esencial para garantizar la seguridad en este ecosistema en constante evolución.

Los niveles de percepción y conocimiento sobre criptomonedas en Colombia evidencian una creciente adopción y aceptación, aunque aún existen mitos y desinformación que pueden influir en la percepción de riesgo de los usuarios. La sugerencia de abordar mitos comunes destaca la persistencia de malentendidos en la sociedad, como la asociación exclusiva de las criptomonedas con actividades ilícitas. La clarificación de estos mitos es esencial para desmitificar la imagen de las criptomonedas y fomentar una comprensión más precisa y equilibrada entre el público en general. Es fundamental que se promueva una educación adecuada y accesible para que los usuarios comprendan tanto los beneficios como los riesgos de esta tecnología. La concienciación y el conocimiento sobre criptomonedas son elementos clave que, al estar fortalecidos, permiten a los usuarios tomar decisiones informadas y reducen la probabilidad de que sean víctimas de amenazas cibernéticas en este ámbito.

La categorización de las estrategias de seguridad en el contexto de blockchain y criptomonedas demuestra que, para mitigar eficazmente las amenazas emergentes, es necesario un enfoque combinado de estrategias técnicas, normativas y de mejores prácticas. Las estrategias técnicas, como el uso de contratos inteligentes seguros y la implementación de autenticación multifactor, deben complementarse con regulaciones claras y educación continua. Este enfoque holístico no solo fortalece la seguridad de las plataformas de blockchain, sino que también fomenta la confianza de los usuarios y el crecimiento seguro del ecosistema de criptomonedas en Colombia.

9 RECOMENDACIONES

Investigar contramedidas específicas para enfrentar amenazas emergentes, como ataques a contratos inteligentes y estafas de inversión en criptomonedas. Las soluciones de seguridad deben adaptarse a las características únicas de este entorno.

Comprender la importancia de proteger la infraestructura de blockchain en sí misma, incluidas las redes y los exchanges. La seguridad en la cadena de bloques es esencial para garantizar la confiabilidad y la integridad de las transacciones.

La adopción de marcos de seguridad como ISO 27001 o el NIST Cybersecurity Framework puede ayudar a las empresas y organizaciones en Colombia a gestionar mejor los riesgos y a implementar medidas de seguridad sólidas en sus operaciones de blockchain.

Las alianzas entre el gobierno, las empresas tecnológicas, y las instituciones financieras son esenciales para compartir información, recursos y estrategias que permitan enfrentar de manera conjunta las amenazas emergentes en el ámbito de blockchain y criptomonedas.

Para proteger la privacidad y la seguridad de las transacciones, se recomienda el uso de algoritmos de cifrado robustos y actualizados. Además, se debe fomentar el uso de técnicas avanzadas para asegurar los datos de los usuarios.

Las plataformas de criptomonedas y blockchain deberían contar con sistemas de monitoreo en tiempo real para detectar y prevenir actividades sospechosas. Estos programas ayudarían a identificar amenazas y a responder rápidamente ante incidentes de seguridad.

Las entidades financieras y los reguladores deberían proporcionar acceso a herramientas que permitan evaluar los riesgos asociados con inversiones en

criptomonedas, ayudando a los usuarios a tomar decisiones informadas y responsables.

La IA puede ayudar a detectar patrones de fraude, ataques de phishing y otros comportamientos anómalos en tiempo real. Incentivar la integración de IA en plataformas de criptomonedas podría fortalecer significativamente la seguridad.

10 BIBLIOGRAFÍA

¿QUÉ ES el cifrado de datos? Definición y explicación [Anónimo]. latam.kaspersky.com [página web]. [Consultado el 11, octubre, 2023]. Disponible en Internet: <https://latam.kaspersky.com/resource-center/definitions/encryption>.

¿QUÉ ES el spyware? - Definición [Anónimo]. latam.kaspersky.com [página web]. [Consultado el 22, octubre, 2023]. Disponible en Internet: <https://latam.kaspersky.com/resource-center/threats/spyware>.

¿QUÉ SON los exchanges de bitcoin y otras criptomonedas? [Anónimo]. CriptoNoticias - Noticias de Bitcoin, Ethereum y criptomonedas [página web]. [Consultado el 23, octubre, 2023]. Disponible en Internet: <https://www.criptonoticias.com/criptopedia/que-son-exchanges-bitcoin-criptomonedas/>.

Â¿QUÃ© ES el doble gasto y por quÃ© supone un problema? [Anónimo]. [Consultado el 22, octubre, 2023]. Disponible en Internet: <https://www.bitpanda.com/academy/es/lecciones/que-es-el-doble-gasto-y-por-que-supone-un-problema/>.

¿CUÁL ES la importancia del Bitcoin? - News America Digital [Anónimo]. News America Digital [página web]. [Consultado el 20, octubre, 2023]. Disponible en Internet: <https://news.america-digital.com/que-es-bitcoin/>.

¿QUÉ ES el malware? Definición y cómo saber si está infectado | Malwarebytes [Anónimo]. Malwarebytes [página web]. [Consultado el 22, octubre, 2023]. Disponible en Internet: <https://es.malwarebytes.com/malware/>.

ESPAÑA, BBVA. ¿Qué es el phishing y cuáles son sus consecuencias? Banco BBVA - Productos financieros para personas y empresas | BBVA [página web]. (9, marzo, 2020). [Consultado el 26, septiembre, 2023]. Disponible en Internet: <https://www.bbva.es/finanzas-vistazo/ciberseguridad/ataques-informaticos/que-es-el-phishing-y-cuales-son-sus-consecuencias.html>.

LAS NFTS, universos digitales (metaverso) y por qué las grandes marcas las están involucrando en sus estrategias de marketing y comercialización. [Anónimo]. Market Team S.A [página web]. [Consultado el 24, septiembre, 2023]. Disponible en Internet: <https://www.linkedin.com/pulse/las-nfts-universos-digitales-metaverso-y-por-qué-grandes-/?originalSubdomain=es>.

SANTANDER. ¿Qué son las criptomonedas y cómo funcionan? Santander Corporate Website [página web]. (12, agosto, 2021). [Consultado el 24, septiembre, 2023]. Disponible en Internet: <https://www.santander.com/es/stories/guia-para-saber-que-son-las-criptomonedas>.

¿CÓMO FUNCIONA un esquema Ponzi? [Anónimo]. BBVA NOTICIAS [página web]. [Consultado el 27, septiembre, 2023]. Disponible en Internet: <https://www.bbva.com/es/como-funciona-un-sistema-ponzi-conocelo-para-protegerte/>.

¿QUÉ ES criptografía? [Anónimo]. NIC Argentina [página web]. [Consultado el 19, octubre, 2023]. Disponible en Internet: <https://nic.ar/es/enterate/novedades/que-es-criptografia#:~:text=La%20criptografía%20es%20el%20desarrollo,no%20estén%20autorizados%20a%20hacerlo.>.

¿QUÉ ES el cifrado de datos? Definición y explicación [Anónimo]. latam.kaspersky.com [página web]. [Consultado el 20, octubre, 2023]. Disponible en Internet: <https://latam.kaspersky.com/resource-center/definitions/encryption>.

¿QUÉ ES el doble gasto? [Anónimo]. Bit2Me Academy [página web]. [Consultado el 26, septiembre, 2023]. Disponible en Internet: <https://academy.bit2me.com/que-es-doble-gasto/>.

¿QUÉ ES el marco de ciberseguridad del NIST? | IBM [Anónimo]. IBM in Deutschland, Österreich und der Schweiz | IBM [página web]. [Consultado el 21, octubre, 2023]. Disponible en Internet: <https://www.ibm.com/mx-es/topics/nist#:~:text=El%20Instituto%20Nacional%20de%20Estándares,la%20tecnología%20de%20la%20medición.>.

¿QUÉ ES el ransomware? | IBM [Anónimo]. IBM in Deutschland, Österreich und der Schweiz | IBM [página web]. [Consultado el 23, octubre, 2023]. Disponible en Internet: <https://www.ibm.com/es-es/topics/ransomware#:~:text=El%20ransomware%20de%20criptomonedas%20comienza,por%20la%20clave%20de%20descifrado.>.

¿QUÉ ES ITIL y para que sirve? [Anónimo]. GlobalSuite Solutions [página web]. [Consultado el 21, octubre, 2023]. Disponible en Internet: <https://www.globalsuitesolutions.com/es/que-es-itil-y-para-que-sirve/>.

¿QUÉ ES la ciberseguridad? - Explicación de la ciberseguridad - AWS [Anónimo]. Amazon Web Services, Inc. [página web]. [Consultado el 1, octubre, 2023]. Disponible en Internet: <https://aws.amazon.com/es/what-is/cybersecurity/#:~:text=La%20ciberseguridad%20es%20la%20práctica,cliente%20y%20cumplir%20la%20normativa.>.

¿QUÉ ES la norma ISO 27001 y para qué sirve? [Anónimo]. GlobalSuite Solutions [página web]. [Consultado el 20, octubre, 2023]. Disponible en Internet: <https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-27001-y-para-que-sirve/>.

¿QUÉ ES la seguridad de blockchain? | IBM [Anónimo]. IBM in Deutschland, Österreich und der Schweiz | IBM [página web]. [Consultado el 20, septiembre, 2023]. Disponible en Internet: <https://www.ibm.com/es-es/topics/blockchain-security#:~:text=IBM-,¿Qué%20es%20la%20seguridad%20de%20blockchain?,riesgos%20contra%20ataques%20y%20fraudes.>.

¿QUÉ ES la tecnología blockchain? - IBM Blockchain | IBM [Anónimo]. Mit watsonx die Leistung der KI multiplizieren | IBM [página web]. [Consultado el 24, septiembre, 2023]. Disponible en Internet: <https://www.ibm.com/es-es/topics/blockchain>.

¿QUÉ ES phishing? - Definición, ejemplos de ataques y más | Proofpoint ES [Anónimo]. Proofpoint [página web]. [Consultado el 22, octubre, 2023]. Disponible en Internet: <https://www.proofpoint.com/es/threat-reference/phishing>.

¿QUÉ ES un adware? [Anónimo]. Argentina.gob.ar [página web]. [Consultado el 22, octubre, 2023]. Disponible en Internet: <https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-un-adware#:~:text=Un%20adware%20es%20un%20tipo,a%20software%20o%20programa%20informático).>.

¿QUÉ ES un ataque DDoS? [Anónimo]. akamai [página web]. [Consultado el 22, octubre, 2023]. Disponible en Internet: <https://www.akamai.com/es/glossary/what-is-ddos>.

¿QUÉ ES un ataque de fuerza bruta? [Anónimo]. latam.kaspersky.com [página web]. [Consultado el 22, octubre, 2023]. Disponible en Internet: <https://latam.kaspersky.com/resource-center/definitions/brute-force-attack>.

¿QUÉ ES un contrato inteligente? - Departamento de Propiedad Intelectual [Anónimo]. Departamento de Propiedad Intelectual [página web]. [Consultado el 25, septiembre, 2023]. Disponible en Internet: <https://propintel.uexternado.edu.co/que-es-un-contrato-inteligente/>.

¿QUÉ ES Un Exchange De Criptomonedas - Bitso Blog [Anónimo]? Bitso Blog [página web]. [Consultado el 21, octubre, 2023]. Disponible en Internet: <https://blog.bitso.com/es-co/criptomonedas-co/que-es-un-exchange-de-criptomonedas>.

¿QUÉ ES un firewall? Definición y explicación [Anónimo]. latam.kaspersky.com [página web]. [Consultado el 20, octubre, 2023]. Disponible en Internet: <https://latam.kaspersky.com/resource-center/definitions/firewall>.

¿QUÉ ES Un Hash Y Cómo Funciona? [Anónimo]. Soluciones de Ciberseguridad Kaspersky para hogar y negocio | Kaspersky | Kaspersky [página web]. [Consultado el 20, octubre, 2023]. Disponible en Internet: <https://latam.kaspersky.com/blog/que-es-un-hash-y-como-funciona/2806/>.

¿QUÉ ES un router? - Definición y usos [Anónimo]. Cisco [página web]. [Consultado el 20, octubre, 2023]. Disponible en Internet: <https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/what-is-a-router.html>.

¿QUÉ ES una criptomoneda y cómo funciona? [Anónimo]. latam.kaspersky.com [página web]. [Consultado el 24, septiembre, 2023]. Disponible en Internet: <https://latam.kaspersky.com/resource-center/definitions/what-is-cryptocurrency>.

¿QUÉ SON los activos digitales y por qué son importantes en tu empresa? [Anónimo]. Consultora Inusual [página web]. [Consultado el 24, septiembre, 2023]. Disponible en Internet: <https://cinusual.com/que-son-los-activos-digitales-y-por-que-son-importantes-en-tu-empresa>.

¿QUÉ SON los activos digitales? Ejemplos y cómo administrarlos [Anónimo]. Xperience Design - Agencia de diseño de servicios [página web]. [Consultado el 25, septiembre, 2023]. Disponible en Internet: <https://www.xperiencedesign.co/blog/qué-son-los-activos-digitales-dos-perspectivas-para-unconcepto#:~:text=Desde%20una%20primera%20perspectiva,%20los,los%20datos%20 recolectados, %20entre%20otros.>.

ACUÑA, Wilder Pereyra. ¿Qué es Blockchain o Tecnología de Registro Distribuido (DLT)? Blog - Escuela Posgrado - Universidad Continental [página web]. (10, mayo, 2022). [Consultado el 24, septiembre, 2023]. Disponible en Internet: <https://blogposgrado.ucontinental.edu.pe/blockchain-tecnologia-registro-distribuid dlt#:~:text=El%20blockchain%20es%20una%20de,ubicaciones%20en %20un%20momento%20dado.>.

AML, QUÉ es y cómo implementarlo en tu negocio | Veridas [Anónimo]. Veridas [página web]. [Consultado el 20, octubre, 2023]. Disponible en Internet: <https://veridas.com/es/que-es-aml/#:~:text=Las%20siglas%20AML%20provienen%20del,que%20proviene%20de %20fuentes%20legítimas.>.

ASÍ VA la Ciberseguridad y su transformación en Latinoamérica [Anónimo]. Certicámara - Entidad pionera en certificación digital en Colombia [página web]. (6,

septiembre, 2019). [Consultado el 22, septiembre, 2023]. Disponible en Internet: <https://web.certicamara.com/files/comdigicert.html>.

ATAQUE DEL 51 % y por qué es importante comprender los modelos de negocio de Blockchain - FourWeekMBA [Anónimo]. FourWeekMBA [página web]. (29, junio, 2023). [Consultado el 25, septiembre, 2023]. Disponible en Internet: <https://fourweekmba.com/es/Ataque-51/>.

ATAQUES A Exchanges de Criptomonedas - Security Art Work [Anónimo]. Security Art Work [página web]. [Consultado el 23, octubre, 2023]. Disponible en Internet: <https://www.securityartwork.es/2022/04/21/ataques-a-exchanges-de-criptomonedas/>.

Binance Academy [página web]. (20, febrero, 2020). [Consultado el 2, octubre, 2023]. Disponible en Internet: <https://academy.binance.com/es/articles/blockchain-scalability-sidechains-and-payment-channels>.

BINANCE COLOMBIA Y la Universidad de los Andes lanzarán cursos sobre Web3 [Anónimo]. BeInCrypto [página web]. [Consultado el 18, octubre, 2023]. Disponible en Internet: <https://es.beincrypto.com/binance-colombia-universidad-andes-lanzaran-cursos-web3/>.

BLOCKCHAIN ¿POR qué y cómo surge? Descúbrelo con Visualeo [Anónimo]. Visualeo [página web]. [Consultado el 19, octubre, 2023]. Disponible en Internet: <https://visualeo.com/blockchian-por-que-y-como-surge/#:~:text=Blockchain%20surge%20en%202008,%20dentro,sistema%20de%20seguridad%20prácticamente%20impenetrable.>.

BLOCKCHAIN SUMMMIT Colombia 2023: Abriendo puertas a la transformación tecnológica - Prensario Tila [Anónimo]. Prensario Tila [página web]. [Consultado el

18, octubre, 2023]. Disponible en Internet: <https://prensariotila.com/blockchain-summmit-colombia-2023-abriendo-puertas-a-la-transformacion-tecnologica/>.

BLOCKCHAIN: QUÉ es la descentralización y qué hay que saber para aprovechar las posibilidades que ofrece [Anónimo]. A24 [página web]. (3, marzo, 2023). [Consultado el 12, septiembre, 2023]. Disponible en Internet: <https://www.a24.com/crypto/blockchain-que-es-la-descentralizacion-y-que-hay-que-saber-aprovechar-las-posibilidades-que-ofrece-n1081251>.

BLOG DE CEUPE. ¿Qué es COBIT? Ceupe [página web]. (27, noviembre, 2018). [Consultado el 21, octubre, 2023]. Disponible en Internet: <https://www.ceupe.com/blog/que-es-cobit.html>.

CAMPAÑA #FAKECOINS: estafas con criptomonedas [Anónimo]. Policía De Investigaciones [página web]. [Consultado el 19, octubre, 2023]. Disponible en Internet: <https://www.pdichile.cl/centro-de-prensa/detalle-prensa/2022/03/30/campaña-fakecoins-estafas-con-criptomonedas>.

CLARKE, Anthony. La tecnología Blockchain mejora la transparencia de las organizaciones benéficas, pero ¿es adecuada para todas? Cointelegraph [página web]. (20, octubre, 2023). [Consultado el 14, septiembre, 2023]. Disponible en Internet: <https://es.cointelegraph.com/news/blockchain-charity-transparency-adoption>.

COLABORADORES DE LOS PROYECTOS WIKIMEDIA. Metaverso - Wikipedia, la enciclopedia libre. Wikipedia, la enciclopedia libre [página web]. (25, mayo, 2007). [Consultado el 24, septiembre, 2023]. Disponible en Internet: <https://es.wikipedia.org/wiki/Metaverso#:~:text=%20En%20la%20novela%20el, aspecto%20de%20la%20realidad%20externa.>.

COLOMBIA ES el tercer país con mayor crecimiento en adopción de criptomonedas en el mundo - Departamento de Derecho Financiero y Bursátil [Anónimo]. Departamento de Derecho Financiero y Bursátil [página web]. [Consultado el 26, septiembre, 2023]. Disponible en Internet: <https://observatoriofinancieroybursatil.uexternado.edu.co/colombia-es-el-tercer-pais-con-mayor-crecimiento-en-adopcion-de-criptomonedas-en-el-mundo/#:~:text=enero%20de%202022-,Colombia%20es%20el%20tercer%20país%20con%20mayor%20crecimiento%20en%20adopción,países%20latinoamericanos%20con%20mayor%20adopción.>.

COLOMBIA FINTECH - Asociación Colombiana de Empresas de Tecnología e Innovación Financiera [Anónimo]. Colombiafintech [página web]. [Consultado el 20, octubre, 2023]. Disponible en Internet: <https://colombiafintech.co/>.

COLOMBIA, EN el 'top' 10 de países con mayor adopción de criptomonedas [Anónimo]. Forbes Colombia [página web]. [Consultado el 26, septiembre, 2023]. Disponible en Internet: <https://forbes.co/2021/03/02/economia-y-finanzas/colombia-en-el-top-10-de-paises-con-mayor-adopcion-de-criptomonedas>.

COLOMBIA: DECRETO 620 de 2020 - Uso y operación de los servicios ciudadanos digitales [Anónimo]. Dentons Cardenas & Cardenas - Home [página web]. [Consultado el 19, octubre, 2023]. Disponible en Internet: <https://dentons.cardenas-cardenas.com/es/insights/articles/2020/may/7/colombia-decree-620-of-2020-use-and-operation-of-digital-citizen-services#:~:text=servicios%20ciudadanos%20digitales-,Colombia:%20Decreto%20620%20de%202020%20-%20Uso%20y%20operación,de%20los%20servicios%20ciudadanos%20digitales&text=El%20Ministerio%20de%20Tecnologías%20de,de%20los%20servicios%20ciudadanos%20digitales.>.

CÓMO COLOMBIA se convirtió en el país de América Latina en el que más crece la compra y venta de bitcoins - BBC News Mundo [Anónimo]. BBC News Mundo [página web]. [Consultado el 10, octubre, 2023]. Disponible en Internet: <https://www.bbc.com/mundo/noticias-america-latina-43219365#:~:text=2017%20fue%20el%20año%20del,transacciones%20hechas%20con%20la%20criptomoneda.>.

CÓMO IDENTIFICAR y prevenir los fraudes de inversiones [Anónimo]. Tennessee State Government - TN.gov [página web]. [Consultado el 23, octubre, 2023]. Disponible en Internet: <https://www.tn.gov/attorneygeneral/working-for-tennessee/consumer/resources/materials/investment-scams-sp.html#:~:text=Los%20fraudes%20de%20inversiones%20consisten,persona%20de%20que%20invierta%20dinero.>.

CRIPTOMONEDAS: ESTO es lo que podría hacer con este tipo de activos [Anónimo]. Portafolio.co [página web]. [Consultado el 22, septiembre, 2023]. Disponible en Internet: <https://www.portafolio.co/economia/finanzas/criptomonedas-como-comenzar-a-invertir-con-divisas-digitales-en-colombia-582785>.

CRIPTO AVANCES. EL IMPACTO DE LAS CRIPTOMONEDAS EN LA SOCIEDAD Y LA ECONOMÍA GLOBAL. LinkedIn: inicio de sesión o registro [página web]. (14, julio, 2023). [Consultado el 19, noviembre, 2023]. Disponible en Internet: <https://es.linkedin.com/pulse/el-impacto-de-las-criptomonedas-en-la-sociedad-y-economía#:~:text=Al%20eliminar%20intermediarios,%20como%20los,y%20tiempos%20de%20espera%20significativamente.>.

CRYPTOJACKING – ¿Qué es y cómo funciona? | Malwarebytes [Anónimo]. Malwarebytes [página web]. [Consultado el 26, septiembre, 2023]. Disponible en

Internet: <https://es.malwarebytes.com/cryptojacking/#:~:text=El%20cryptojacking%20es%20una%20forma,monedas%20online%20como%20el%20bitcoin.>.

CUÁNTO INVIERTEN los colombianos en criptomonedas y con qué fin [Anónimo]. Portafolio.co [página web]. (21, marzo, 2023). [Consultado el 22, septiembre, 2023]. Disponible en Internet: <https://www.portafolio.co/economia/finanzas/criptomonedas-en-colombia-cuanto-invierten-en-esos-activos-los-colombianos-580173>.

DECRETO 1074 de 2015 [Anónimo]. MINTIC [página web]. [Consultado el 19, octubre, 2023]. Disponible en Internet: <https://www.mincit.gov.co/ministerio/normograma-sig/procesos-misionales/facilitacion-del-comercio-y-defensa-comercial/decretos/2015/decreto-1074-de-2015-1.aspx>.

DLT/BLOCKCHAIN [Anónimo]. mintic.gov.co [página web]. [Consultado el 25, septiembre, 2023]. Disponible en Internet: <https://mintic.gov.co/portal/715/articles-149959_recurso_1.pdf>.

EL CONFIDENCIAL - El diario de los lectores influyentes [Anónimo]. elconfidencial.com [página web]. [Consultado el 27, septiembre, 2023]. Disponible en Internet: <https://www.elconfidencial.com/>.

EL WHITEPAPER de Bitcoin ha sido traducido a más de 40 idiomas [Anónimo]. Bit2Me News | Noticias cripto, Blockchain, Ethereum [página web]. [Consultado el 19, octubre, 2023]. Disponible en Internet: <https://news.bit2me.com/whitepaper-de-bitcoin-traducido-a-mas-de-40-idiomas/#:~:text=En%20octubre%20de%202008,%20Satoshi,la%20autorización%20de%20una%20entidad>.

EMPEY, Charlotte y LATTO, Nica. ¿Qué es una VPN y cómo funciona? ¿Qué es una VPN y cómo funciona? [página web]. (8, abril, 2020). [Consultado el 20, octubre, 2023]. Disponible en Internet: <https://www.avast.com/es-es/c-what-is-a-vpn>.

ESTAS SON las siete dudas legales sobre el uso de los criptoactivos y su regulación [Anónimo]. Noticias de Abogados, bufetes, jurisprudencia, avisos de ley, de Colombia| Asuntoslegales.com.co [página web]. [Consultado el 19, octubre, 2023]. Disponible en Internet: <https://www.asuntoslegales.com.co/actualidad/estas-son-las-siete-dudas-legales-sobre-el-uso-de-los-criptoactivos-y-su-regulacion-3155325>.

FERNÁNDEZ, Yúbal. Bitcoin, guía a fondo: qué es, cómo funciona y cómo conseguirlos. Xataka - Tecnología y gadgets, móviles, informática, electrónica [página web]. (9, junio, 2023). [Consultado el 20, octubre, 2023]. Disponible en Internet: <https://www.xataka.com/basics/bitcoin-guia-a-fondo-que-como-funciona-como-conseguirlos>.

GESTIÓN DE riesgos emergentes: cómo identificar amenazas de baja probabilidad y alto impacto a tiempo [Anónimo]. Escuela Europea de Excelencia [página web]. [Consultado el 24, septiembre, 2023]. Disponible en Internet: <https://www.escuelaeuropeaexcelencia.com/2022/03/gestion-de-riesgos-emergentes-como-identificar-amenazas-de-baja-probabilidad-y-alto-impacto-a-tiempo/>.

GUÍA PARA madres, padres, familias y docentes: amenazas en internet [Anónimo]. Argentina.gob.ar [página web]. [Consultado el 21, octubre, 2023]. Disponible en Internet: <https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/guia-para-madres-padres-docentes-amenazas-internet#:~:text=Es%20todo%20lo%20que%20atenta,actividades%20por%20medio%20de%20internet.>.

GUÍA PRÁCTICA sobre el tratamiento legal de las Criptomonedas en Colombia: Recomendaciones y reflexiones [Anónimo]. Centro de Estudios Regulatorios [página web]. [Consultado el 26, septiembre, 2023]. Disponible en Internet: <https://www.cerlatam.com/publicaciones/guia-practica-sobre-el-tratamiento-legal-de-las-criptomonedas-en-colombia-recomendaciones-y-reflexiones/#:~:text=El%20proyecto%20de%20ley%20268%20de%202019.,de%20moneda%20de%20curso%20legal.>.

IBERDROLA. Ciberataques. Iberdrola [página web]. (30, junio, 2021). [Consultado el 25, septiembre, 2023]. Disponible en Internet: <https://www.iberdrola.com/innovacion/ciberataques>.

IC Y Blockchain: retos y riesgos - OpenMind [Anónimo]. OpenMind [página web]. [Consultado el 19, septiembre, 2023]. Disponible en Internet: <https://www.bbvaopenmind.com/tecnologia/futuro/ic-y-blockchain-retos-y-riesgos/>.

INGENIERÍA SOCIAL: qué es y cómo prevenirla | Click-IT | Servicios tecnológicos y de consultoría [Anónimo]. Click-IT | Servicios tecnológicos y de consultoría | [página web]. [Consultado el 22, octubre, 2023]. Disponible en Internet: <https://click-it.es/ingenieria-social-que-es-y-como-prevenirla/>.

LA HISTORIA de Ethereum | Plus500 [Anónimo]. Online-CFD-Handel | Mit den Märkten handeln | Plus500 [página web]. [Consultado el 19, octubre, 2023]. Disponible en Internet: <https://www.plus500.com/es/Instruments/ETHUSD/The-History-of-Ethereum~4#:~:text=Creación%20de%20Ethereum&text=En%202015,%20después%20de%20una,sistema%20para%20abril%20de%202020.>.

LAS AMENAZAS emergentes en seguridad: Cryptomining, SASE - PrensarioHub [Anónimo]. PrensarioHub [página web]. [Consultado el 27, septiembre, 2023]. Disponible en Internet: <https://www.prensariohub.com/las-amenazas-emergentes-en-seguridad-cryptomining.

LAS CRIPTOMONEDAS mueven $70.000 millones en transacciones en Colombia [Anónimo]. Semana.com Últimas Noticias de Colombia y el Mundo [página web]. (12, julio, 2022). [Consultado el 26, septiembre, 2023]. Disponible en Internet: <https://www.semana.com/economia/capsulas/articulo/las-criptomonedas-mueven-70000-millones-en-transacciones-en-colombia/202226/>.

LAS SOLUCIONES de ciberseguridad que deberían priorizar las empresas este 2023 - Prensario Tila [Anónimo]. Prensario Tila [página web]. [Consultado el 26, septiembre, 2023]. Disponible en Internet: <https://prensariotila.com/las-soluciones-de-ciberseguridad-que-deberian-priorizar-las-empresas-este-2023/>.

LEGALIDAD DE las Criptomonedas: Avance significativo en la economía digital de Colombia - Blog Jurídico - TECH [Anónimo]. Blog Jurídico - TECH [página web]. [Consultado el 26, septiembre, 2023]. Disponible en Internet: <https://telecomunicaciones.uexternado.edu.co/legalidad-de-las-criptomonedas-avance-significativo-en-la-economia-digital-de-colombia/#:~:text=Más%20adelante,%20el%20presidente%20Luiz,junio%20del%202023[5].>.

LEY 1273 de 2009 -Legislacion Colombiana Lexbase [Anónimo]. INFORMACION JURIDICA, BASE DE DATOS ESPECIALIZADA , BASE DE DATOS JURIDICA LEXBASE - COLOMBIA [página web]. [Consultado el 20, octubre, 2023]. Disponible en Internet: <https://www.lexbase.co/lexdocs/indice/2009/l1273de2009#:~:text="%20LEY%201273%20DE%202009%20(enero,y%20las%20comunicaciones,%20entre%20otras>

LOS MONEDEROS de criptomonedas físicos y digitales: ¿qué son y cómo se roban? [Anónimo]. Soluciones de ciberseguridad de Kaspersky para hogares y empresas | Kaspersky [página web]. [Consultado el 23, octubre, 2023]. Disponible en Internet: <https://www.kaspersky.es/blog/five-threats-hardware-crypto-wallets/28724/>.

MALWARE DE extracción de criptomonedas (cryptojacking): qué es y cómo protegerse | ESET [Anónimo]. Malware Protection & Internet Security | ESET [página web]. [Consultado el 26, septiembre, 2023]. Disponible en Internet: <https://www.eset.com/co/malware-extraccion-cryptomonedas/>.

MCAFEE. ¿Qué es el malware? | McAfee. McAfee [página web]. (15, mayo, 2020). [Consultado el 20, octubre, 2023]. Disponible en Internet: <https://www.mcafee.com/es-mx/antivirus/malware.html#:~:text=Malware%20es%20un%20término%20que,víctimas%20para%20obtener%20ganancias%20financieras.>.

MORALES, Carlos Rodríguez. Blockchain y ciberseguridad: la inmutabilidad (II). Telefónica Tech [página web]. (19, septiembre, 2019). [Consultado el 14, septiembre, 2023]. Disponible en Internet: <https://telefonicatech.com/blog/blockchain-y-ciberseguridad-la-inmutabilidad#:~:text=La%20inmutabilidad,%20la%20capacidad%20para,destaca%20como%20un%20beneficio%20clave.>.

MONERO, ZCASH y Dash, las mejores criptomonedas anónimas [Anónimo]. Businessinsider [página web]. [Consultado el 19, noviembre, 2023]. Disponible en Internet: <https://www.businessinsider.es/cripto/noticias/monero-zcash-dash-mejores-criptomonedas-anonimas/>.

PARCHES DE Seguridad y Actualizaciones | BCSC [Anónimo]. Inicio | BCSC [página web]. [Consultado el 20, octubre, 2023]. Disponible en Internet: <https://www.ciberseguridad.eus/ciberpedia/buenas-practicas/parches-de-seguridad-y-actualizaciones#:~:text=Un%20parche%20de%20seguridad%20o,de%20actualizaciones%20o%20nuevas%20versiones.>.

POLÍTICA DE Protección de Datos Personales - Ministerio de Ambiente y Desarrollo Sostenible [Anónimo]. Ministerio de Ambiente y Desarrollo Sostenible [página web]. [Consultado el 20, octubre, 2023]. Disponible en Internet: <https://www.minambiente.gov.co/politica-de-proteccion-de-datos-personales/#:~:text=Ley%20de%20Protección%20de%20Datos,de%20naturaleza%20pública%20o%20privada.>.

QUÉ ES Bitcoin: origen, usos, ventajas y riesgos [Anónimo]. LISA Institute [página web]. [Consultado el 19, octubre, 2023]. Disponible en Internet: <https://www.lisainstitute.com/blogs/blog/que-es-bitcoin-origen-usos-ventajas-riesgos#:~:text=En%20enero%20de%202009%20entró,divisas%20como%20medio%20de%20pago.>.

QUE SON las DLT y en que se diferencian de Blockchain [Anónimo]. Thinking for Innovation [página web]. [Consultado el 24, septiembre, 2023]. Disponible en Internet: <https://www.iebschool.com/blog/que-son-las-dlt-y-en-que-se-diferencian-de-blockchain-digital-business/>.

QUÉ SON los contratos inteligentes [Anónimo]. CriptoNoticias - Noticias de Bitcoin, Ethereum y criptomonedas [página web]. [Consultado el 24, septiembre, 2023]. Disponible en Internet: <https://www.criptonoticias.com/criptopedia-old/que-son-contratos-inteligentes-blockchain-criptomonedas/>.

QUÉ SON y cómo funcionan los ataques de suplantación de identidad [Anónimo]. EALDE Business School [página web]. [Consultado el 23, octubre, 2023]. Disponible en Internet: <https://www.ealde.es/ataques-de-suplantacion-de-identidad/>.

ROBO DE identidad [Anónimo]. SEON ES [página web]. [Consultado el 23, octubre, 2023]. Disponible en Internet: <https://seon.io/es/recursos/glosario/que-es-el-robo-de-identidad/#:~:text=El%20robo%20de%20identidad%20es,verdadera%20identidad%20de%20los%20estafadores.>.

SEGURIDAD DE Criptomonedas: 3 Claves Para Protegerlas - Bitso Blog [Anónimo]. Bitso Blog [página web]. [Consultado el 23, octubre, 2023]. Disponible en Internet: <https://blog.bitso.com/es-ar/seguridad-ar/seguridad-de-criptomonedas#:~:text=Implica%20tomar%20medidas%20para%20proteger,más%20popularidad%20entre%20los%20inversores.>.

SEGURIDAD DE Criptomonedas: 3 Claves Para Protegerlas - Bitso Blog [Anónimo]. Bitso Blog [página web]. [Consultado el 23, octubre, 2023]. Disponible en Internet: <https://blog.bitso.com/es-ar/seguridad-ar/seguridad-de-criptomonedas#:~:text=Implica%20tomar%20medidas%20para%20proteger,más%20popularidad%20entre%20los%20inversores.>.

SEGURIDAD INFORMÁTICA: La importancia y lo que debe saber [Anónimo]. Educación Sin Fronteras | UdeCataluña [página web]. [Consultado el 24, septiembre, 2023]. Disponible en Internet: <https://www.ucatalunya.edu.co/blog/seguridad-informatica-la-importancia-y-lo-que-debe-saber>.

STABLECOIN: QUÃ© es una moneda estable / Buda.com [Anónimo]. Buda.com - Compra Bitcoin y Ethereum en Chile [página web]. [Consultado el 20, octubre,

2023]. Disponible en Internet: <https://www.buda.com/guias/stablecoin#:~:text=Una%20stablecoin%20es%20una%20criptomoneda,,%20euro,%20etc.).>.

VIRUS INFORMÁTICO - Tecnología | Uniandes [Anónimo]. Tecnología | Uniandes [página web]. [Consultado el 20, octubre, 2023]. Disponible en Internet: <https://tecnologia.uniandes.edu.co/virus-informatico/>.

VULNERABILIDAD [Anónimo]. Banco Santander [página web]. [Consultado el 20, octubre, 2023]. Disponible en Internet: <https://www.bancosantander.es/glosario/vulnerabilidad-informatica#:~:text=En%20informática,%20una%20vulnerabilidad%20es,malintencionada%20para%20comprometer%20su%20seguridad.>.

WHAT IS the block height? [Anónimo]. Bit2Me Academy [página web]. [Consultado el 20, octubre, 2023]. Disponible en Internet: <https://academy.bit2me.com/en/what-is-block-height/>.