TRABAJO DE GRADO
Opción Seminario-Diplomado

Seguridad Transaccional en Blockchain

Corporación Universitaria Remington
Facultad de ingenierías
Seminario Blockchain

Juan Andrés Hernández Uñates
Frank Humberto Cabrera Lerma
Donnadonis guerrero Hernández

Juan Pablo Vélez Uribe.
Opción de Trabajo de grado Seminario-Diplomado
2024.

Dedicatoria

Especialmente dedicado a todas nuestras familias. Realizado con un gran esfuerzo y dedicación que nos ha permitido llegar hasta este punto, construyendo bases de conocimiento solidas que nos han aportado un gran crecimiento personal y profesional, con la finalidad de hacer aportes positivos a la sociedad.

Agradecimientos

Especial agradecimiento para nuestros padres y hermanos por el apoyo y confianza brindados, y a la Corporación Universitaria Remington, que nos ha permitido desarrollar conocimientos, habilidades y destrezas en el proceso académico virtual de las carreras de Ingeniería industrial e Ingeniería de sistemas, las cuales son de vital importancia para generar valor a la sociedad por medio de sus egresados.

Tabla de Contenido

Resumen 7

Palabras Clave 7

Marco Conceptual 8

Marco Contextual 12

Objetivo General 12

Objetivos específicos 12

Contexto 12

Desarrollo e Implementación del Aprendizaje 14

Transacciones en Blockchain 15

Transacciones en Bitcoin 16

Seguridad en Blockchain 19

Conceptos de Criptografía en Blockchain 19

Primitivas criptográficas sin clave 20

Criptografía Simétrica 21

Criptografía de Clave Asimétrica 21

Proof of Work o Prueba de Trabajo 22

Firmas Digitales 22

Árbol de Merkle 22

Contratos inteligentes en Blockchain 23

Blockchain Dapps 25

Conclusiones 27

Referencias 29

Tabla de ilustraciones

Figura 1. Fase de la evolución de la tecnología de Blockchain. 10

Figura 2. Clasificación de Blockchain por Nivel de Permisos y Escalabilidad. 14

Figura 3. Proceso de Transacciones en Blockchain. 16

Figura 4. Procesos en una transacción de la red Bitcoin. 18

Figura 5. Criptografía simétrica. 19

Figura 6. Algoritmo del Hash. 21

Figura 7. Explicación de contrato inteligente. 23

Figura 8. Auditoria de un Smart Contract. 26

Resumen

La finalidad de este documento es analizar, a partir de criterios investigativos, conceptos, estándares y recomendaciones internacionales, el impacto de la tecnología Blockchain en la actualidad y más precisamente su seguridad, sus estrategias y metodologías aplicadas para mitigar las dificultades a nivel de seguridad transaccional. Para tal fin, este trabajo presenta un desarrollo a partir de conceptos básicos que permiten una inmersión en el tema de manera técnica y clara. Blockchain ya existe hace aproximadamente 16 años y sus niveles de seguridad han presentado actualizaciones y mejoras precisamente por la necesidad de proteger la información. Aquí también se explicará por qué Blockchain es uno de los sistemas más seguros. Se definirá y contextualizara de que se trata y cómo funciona este sistema que se viene implementando, actualizando y adoptando por diferentes tipos de organizaciones a nivel global.

La investigación incluye temáticas referentes a las transferencias y la seguridad que las acompaña internamente en todo el flujo del proceso. La criptografía, el hash, los Smart Contracts y otras técnicas de seguridad serán objeto de estudio para crear una base sólida de conocimiento sobre esta tecnología que se está fortaleciendo cada vez más.

Palabras Clave

Blockchain, Seguridad, Transacciones, eficiencia, criptomonedas, Smart Contracts, Descentralización, Minería, Privacidad, Transparencia.

Marco Conceptual

Antes de desarrollar el tema formalmente, es conveniente la introducción de algunos conceptos básicos para el correcto entendimiento de todo lo relacionado con Blockchain:

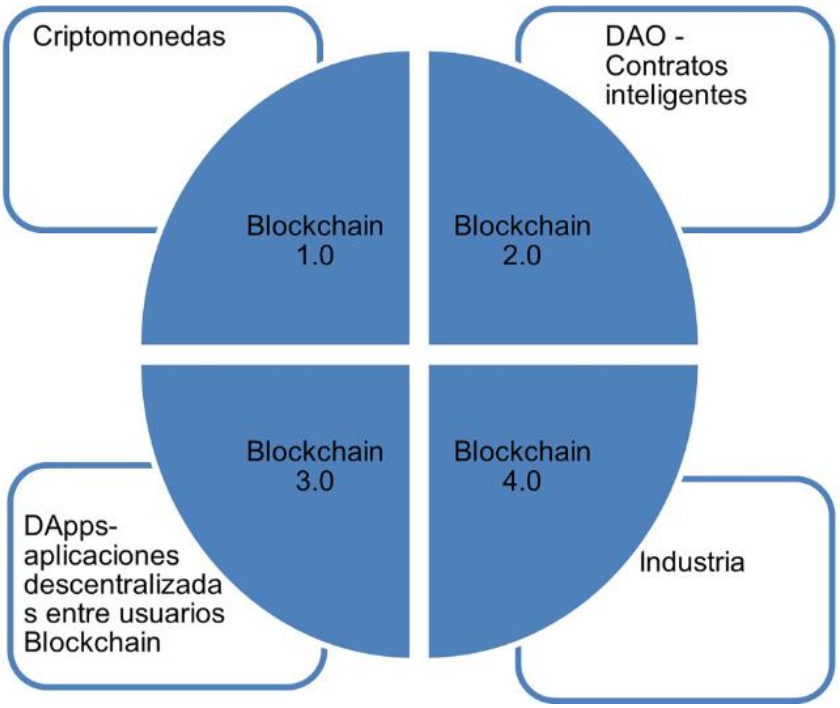
- **Nodo:** La Blockchain es una red que se compone de nodos. Los nodos son dispositivos digitales o computadoras que se encuentran interconectadas por el mismo software para poder transar.
- **Nodo minero:** Son los nodos que verifican e ingresan las transacciones en bloques a la Blockchain. Por su trabajo como mineros reciben recompensas que normalmente es entregada en criptomonedas.
- **Hash:** El hash es un algoritmo matemático que recibe datos de entrada y la convierte en una nueva serie de caracteres.
- **Bloque:** Los bloques son estructuras que almacenan información. Cada nodo posee bloques con la información exacta y todos los nodos tienen acceso a ella.
- **Proof of Work:** Es el proceso de producción de los bloques. Es un proceso donde se debe resolver un problema matemático para poder añadir un nuevo bloque a la cadena.
- **Descentralización:** Es otorgar el control y la toma de decisiones a toda la red y no a un ente central como por ejemplo un banco.

En 2008 Nakamoto hizo la publicación que conceptualizó la famosa criptomoneda llamada Bitcoin y la forma en que su funcionamiento se basaba en las características del Blockchain (Noriega, 2022). El Blockchain o cadena de bloques es una tecnología que almacena registros de forma descentralizada e inmutable, lo que abre una infinidad de posibles formas de aplicación en distintas disciplinas y sectores empresariales. Esta tecnología, entre tantos beneficios que la componen, cuenta con uno muy relevante que es la capacidad de llevar un

registro controlado de cualquier cosa de valor, esto permite disminuir costos y riesgos para todas las partes. Parte de la seguridad de la Blockchain se basa en la encriptación de la información y su organización en bloques (Mithuyoshi y Sánchez 2023).

Con la llegada del Bitcoin, que no era otra cosa que una moneda digital que permitía realizar transacciones entre usuarios por medio de un computador o un dispositivo con un software especifico, se generó la necesidad de incrementar la seguridad sobre las operaciones que se realizaban aplicando técnicas de criptografía y usando las tecnologías de redes vigentes en la época. Con el paso de los años y hasta el presente, se han generado diferentes necesidades referentes a la seguridad transaccional y no solo sobre lo relacionado con las criptomonedas, ya que Blockchain tiene aplicaciones en la industria financiera, administración, sistemas de elecciones, residencia e identificación electrónica, justicia, arte, medio ambiente, salud, y entre otras que de forma imperativa han generado la necesidad de implementar un riguroso sistema de seguridad transaccional bajo los principios de la incorruptibilidad y la privacidad. Actualmente Blockchain guarda registro de cada transacción y la distribuye a cada usuario de la red, permitiendo generar un historial similar a un libro contable donde todos los usuarios tienen acceso de forma pública (Arteaga, D. & Pantoja, L. 2022).

Figura 1. Fase de la evolución de la tecnología de Blockchain.



Nota: Esta figura representa la evolución del Blockchain y sus diferentes etapas de desarrollo a lo largo del tiempo. *Tomado de: Pereira C. (2022). Fuente:* https://www.scielo.br/j/tinf/a/PJWKFWfCxGNHbLdxtzLP9nB/

Según (Romero, et al. 2023), la tecnología Blockchain no es una empresa, ni tampoco es un producto, sino un software tipo plataforma tecnológica que brinda muchos beneficios enfocados en la seguridad transaccional y permite operar de forma descentralizada. La cadena de bloques es una red que no es regulada por una entidad central, sino que a través de los nodos de la misma red se distribuye la información para todos los usuarios. La toma de decisiones en Blockchain depende directamente de un sistema de consenso, el cual requiere que por lo menos el 51% de los nodos coincidan en la información que comparten. La seguridad del Blockchain en gran parte depende del mecanismo llamado *Proof of Work*, que es una combinación de criptografía y técnicas de computación que crean consenso y aseguran la autenticidad de la

información. Para validar que un bloque de información es correcto, los nodos mineros, por medio de su poderoso hardware, validan las transacciones, en caso de bitcoin, verifican que el remitente tenga suficientes fondos para transar y que no se realice doble gasto. Y lo más importante, los mineros compiten entre ellos mismos para lograr resolver el problema criptográfico y poder obtener su recompensa (Seang, S., & Torre, D., 2018).

Entre los retos más desafiantes que afronta Blockchain, existen dos que son bastante preocupantes e impiden la evolución y crecimiento de la tecnología debido a su nivel de complejidad. El primero de ellos es la gran cantidad de energía eléctrica que requiere un nodo minero para poder instalar su complejo equipo de hardware y poder realizar sus labores de minado; por esta misma razón, los mineros buscan regiones donde los costos de energía eléctrica no sean tan elevados y así poder realizar sus labores a bajo costo. El segundo reto que afronta esta tecnología es su baja velocidad de operación comparada con otras tecnologías que son bastante fuertes en este aspecto. Por ejemplo: Blockchain tiene la capacidad de realizar entre 55 a 120 operaciones por segundo, sin embargo, la franquicia Visa que se dedica a la intermediación de transferencias de fondos por medio de tarjetas de crédito y débito, alcanza la enorme cantidad de 70.000 transacciones por segundo, lo cual es aproximadamente 804 veces más de lo que logra Blockchain.

Marco Contextual

Objetivo General

Realizar una investigación basada en artículos científicos e información certificada sobre la seguridad en las transacciones de Blockchain. Iniciando con los conceptos básicos que componen la tecnología y luego detallar algunos de los principales métodos que garantizan la seguridad de las transacciones en la plataforma.

Objetivos específicos

- Introducir conceptos básicos de Blockchain.
- Investigar las aplicaciones más importantes de esta tecnología.
- Definir el concepto de transacción en Blockchain.
- Investigar los conceptos principales de la seguridad en Blockchain enfocados a la transaccionalidad.

Contexto

El presente marco contextual tiene como objetivo analizar la seguridad transaccional en Blockchain, abordando los principales desafíos y oportunidades que esta tecnología ofrece en la seguridad de las transacciones digitales. Blockchain es una tecnología que garantiza la seguridad de las transacciones a través de registros distribuidos y descentralizados. Desde su aparición en 2008, Blockchain ha evolucionado para convertirse en una solución para la protección de transacciones digitales, especialmente en el ámbito financiero. Al utilizar contratos inteligentes, el sistema de cadena de bloques permite que estas transacciones se automaticen, por ende, las hace seguras, reduciendo la posibilidad de fraudes (Dai, Lu, & Huang, 2024).

Blockchain es una tecnología de contabilidad distribuida que se caracteriza por su resistencia a la manipulación, descentralizada, inmutable y que permite la trazabilidad, considerada una innovación tecnológica revolucionaria.

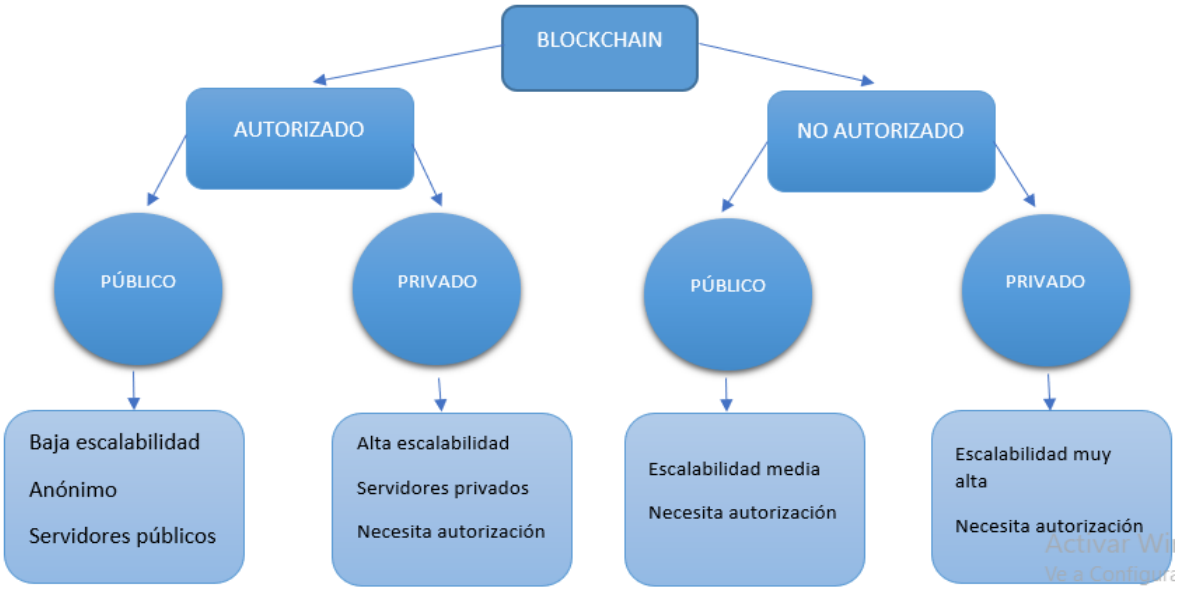
La protección de datos y criptomonedas, son factores de suma importancia al adquirir Blockchain ya que este impacta en la confianza de los usuarios, comprender en cómo funciona o como opera la seguridad transaccional en Blockchain es esencial y de suma importancia para evaluar su eficacia y potencial en diversas aplicaciones.

Blockchain es una tecnología que elimina intermediarios en las transacciones digitales al utilizar una red distribuida, lo que refuerza la seguridad al dificultar ataques y manipulaciones por personas inescrupulosas (Nakamoto, 2008; Conti et al., 2018).

A pesar de sus ventajas, uno de los desafíos principales es la escalabilidad, ya que el manejo de grandes volúmenes de transacciones puede comprometer la eficiencia.

Además del sector financiero, Blockchain se ha expandido a áreas como la cadena de suministro, la salud y la votación electrónica, donde la seguridad transaccional es crucial para mantener la integridad de los datos y la confianza de los usuarios (Tapscott & Tapscott, 2017). A largo plazo, el éxito de Blockchain dependerá de su capacidad para resolver desafíos de escalabilidad, privacidad y regulación, mientras se aprovechan sus características de transparencia e inmutabilidad a través de contratos inteligentes, estos contratos inteligentes son de demasiada importancia ya que estos contratos, se pueden automatizar, y estos se finalizarán una vez se cumpla todo lo pactado.

Figura 2. Clasificación de Blockchain por Nivel de Permisos y Escalabilidad.



Nota: Este esquema hace referencia a los tipos de red de Blockchain para ser usadas en contextos específicos. *Tomado de: Softtek (2018). Recuperado el 13 de septiembre de 2024. Fuente:* https://blog.softtek.com/es/el-70-del-valor-del-blockchain-reside-en-la-reduccion-de-los-costes.

Desarrollo e Implementación del Aprendizaje

La construcción del conocimiento en este trabajo está basada en investigación hecha en bases de datos científicas certificadas sobre la terminología básica usada en la tecnología Blockchain para conformar la parte conceptual, y después continuar con el desarrollo de un estudio detallado sobre los temas relacionados con las transacciones que se realizan en la cadena de bloques a nivel general sobre cualquiera de sus aplicaciones o disciplinas, y por ultimo estudiar algunos métodos para garantizar la seguridad y buenas prácticas para la seguridad.

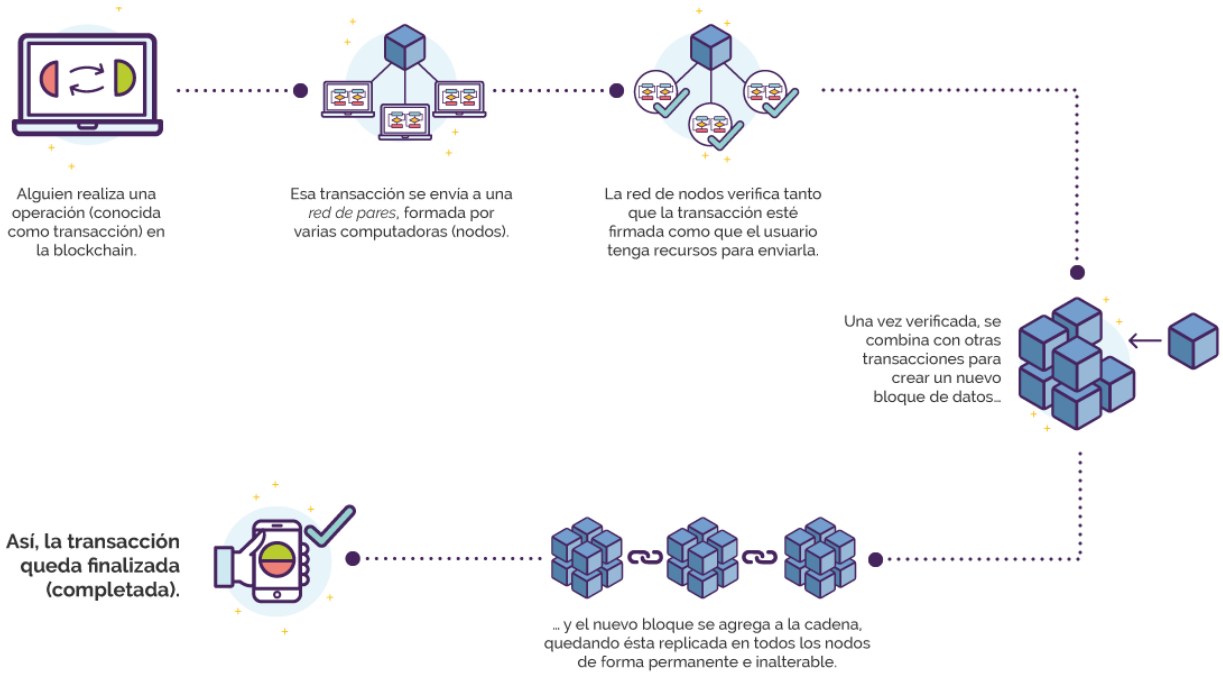
En este informe, presento los resultados de la implementación de lo aprendido en el cursor de seguridad transaccional en Blockchain, en el contexto de un proyecto de desarrollo de una

plataforma de intercambio de criptomonedas. Se analizarán los detalles técnicos de la implementación y se evaluarán los resultados obtenidos.

Transacciones en Blockchain

Blockchain desde su nacimiento y por su divulgación, lo conciben como una tecnología ligada generalmente a Bitcoin. Por esta razón, es muy usual asociar la palabra transacción a la acción de mover fondos o dinero de un usuario a otro dentro de la aplicación de Bitcoin. Y esto realmente si es una transacción. Pero "transacción" es una palabra que dentro de Blockchain tiene una definición mucho más amplia y generalizada que no está ligada directamente al ámbito financiero. Según IBM (*What is blockchain?*, 2023), las transacciones de la red pueden ser tangibles o intangibles, es decir, puede ser un producto físico o una propiedad intelectual respectivamente. Estas transacciones se registran como un bloque de datos, donde se puede almacenar datos adicionales de forma opcional como, por ejemplo: ¿qué?, ¿quién?, ¿cuándo?, ¿dónde? ¿Y cuánto?, incluso algunos datos adicionales. Los bloques que se van creando quedan inmediatamente asociados al bloque anterior, lo que hace que toda la cadena se vaya fortaleciendo, creando su carácter de inmutabilidad y eliminando la posibilidad de llegar a ser manipulada por terceros malintencionados.

Figura 3. Proceso de Transacciones en Blockchain.



NOTA: Esta grafica muestra el proceso de transacciones en Blockchain asegurándose de que se cumplan las reglas y condiciones de transacción. *Tomado de: Blockchain Federal Argentina. Bloques y transacciones (s/f). Recuperado el 13 de septiembre de 2024, de https://bfa.ar/blockchain/bloques-y-transacciones*

Transacciones en Bitcoin

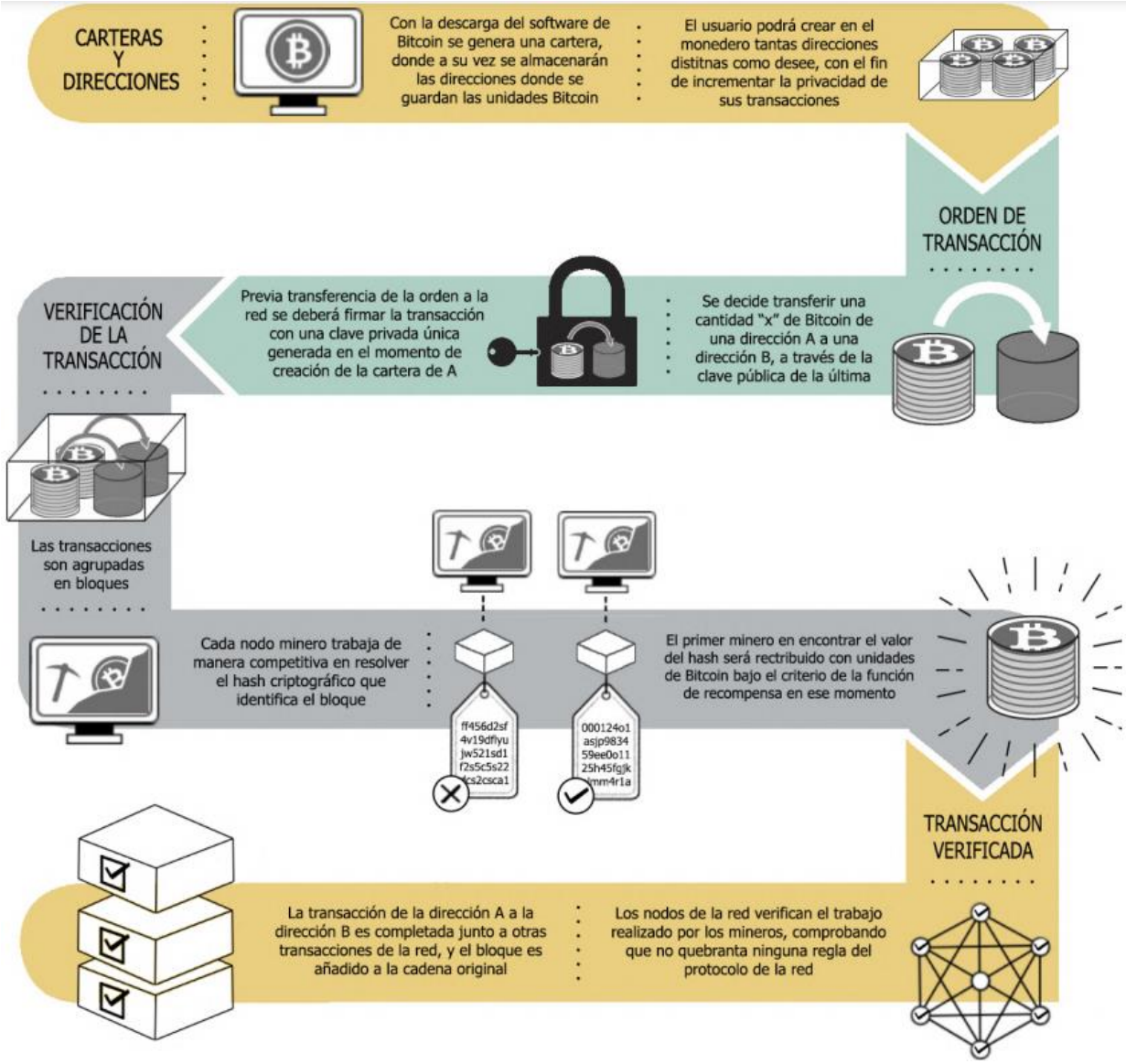
Bitcoin es una forma diferente de ver el dinero y usarlo de forma descentralizada, sin necesidad de acudir a entidades bancarias o intermediarios en los movimientos financieros que se deseen realizar. Las transacciones en bitcoin se basan en procesos clave como la información, verificación y minado. Gracias a Blockchain, bitcoin almacena todas las transacciones realizadas, que corresponden a movimientos de saldos de bitcoin de un usuario a otro.

La creación de nuevos bloques es una tarea que se asigna exclusivamente a los nodos mineros, y son ellos precisamente quienes, por medio de tecnología bastante poderosa y costosa,

se dedican a resolver acertijos matemáticos para la validación de los nuevos bloques de la cadena, lo cual genera incentivos a manera de recompensa para el primero que logre resolver el complicado acertijo matemático. Es importante mencionar que la aparición de nuevos Bitcoin es gracias a las recompensas que se asignan a los nodos mineros ya que cada vez que se incentiva a un minero por su logro, los Bitcoin que adquiere son de nueva creación. Las recompensas suministradas disminuyen un 50% cada 210.000 bloques.

Por otro lado, descargar el software de Bitcoin, es lo que permite al usuario empezar a usar la cartera y almacenar su saldo, convirtiéndose automáticamente en un nodo. Todos los nodos de forma natural tienen su cartera asociada. Estas carteras vienen dotadas con una dirección única para cada una que funciona similar a un número de cuenta o identificación, sin embargo, para efectuar una transacción hace falta más que ese número de identificación, ya que el remitente, por medio de sus claves privadas, debe firmar la operación como señal de aceptación (Rodriguez Gomez et al., 2020).

Figura 4. Procesos en una transacción de la red Bitcoin.



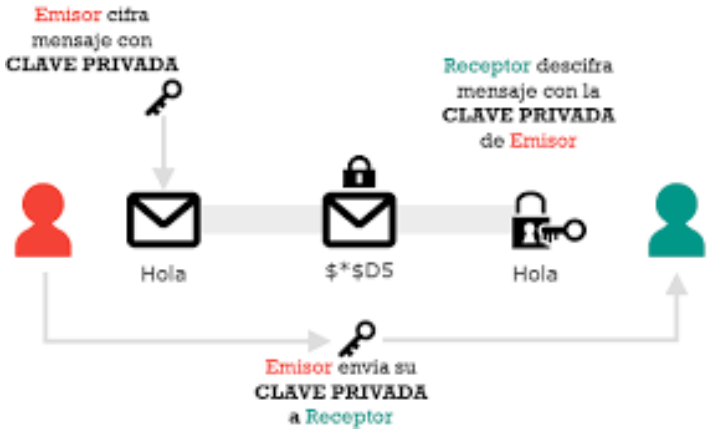
Nota: Este grafico representa el proceso detallado de una transacción en Bitcoin desde la descarga del software hasta que el destinatario recibe la transferencia. Tomado de Rodríguez Gómez et al. (2020). Bitcoin, un activo de inversión alternativo. Fuente: *https://ruc.udc.es/dspace/bitstream/handle/2183/26065/RodriguezGomez_JoseLuis_TFM_2020.pdf?sequence=2&isAllowed=y*

Seguridad en Blockchain

Conceptos de Criptografía en Blockchain

La criptografía utiliza las matemáticas para cifrar o descifrar información dependiendo de la necesidad y el contexto. Su uso se basa en la necesidad de "disfrazar" la información para luego enviarla al interesado y que pueda ser descifrada e interpretada según el mensaje original. Además de transmitir un mensaje de un individuo A hacia un individuo B, también protege la información de terceros a quienes no va dirigida la información. A nivel técnico la criptografía usa algoritmos basados en métodos matemáticos que permiten que la comunicación entre las partes interesadas sea efectiva y segura a través de un canal inseguro, garantizando privacidad y autenticidad (Gómez, 2023).

Figura 5. Criptografía simétrica.



Nota: En esta figura muestra el funcionamiento de la criptografía. *Tomado de: Asixasantamaria (2019). Recuperado el 13 de septiembre del 2024. Fuente https://ciberseguridadasix.wordpress.com/2019/02/26/criptografia-simetrica/*

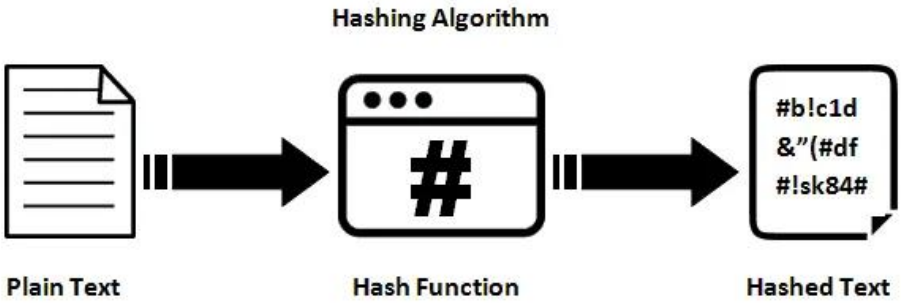
Primitivas criptográficas sin clave

Secuencias Aleatorias. La criptografía requiere una gran cantidad de secuencias aleatorias ya sea para los procesos de cifrado o para la generación de claves. Estas secuencias aleatorias no deben ser previsibles. Existen dos generadores de números aleatorios: el sistema TRNG y el sistema PRNG.

- **Sistema TRNG:** Es un Hardware que genera números que no se pueden adivinar y se basa en variables físicas externas para ser realmente aleatorio.
- **Sistema PRNG:** Es un algoritmo que genera números aleatorios a partir de funciones estadísticas.

Funciones Hash. La función Hash son métodos que se usan para convirtiendo un conjunto de datos de entrada en un dato de salida hash. Solo funciona en una dirección, es decir que funciona convirtiendo datos en Hash, pero no tomando un Hash y volviendo a los datos iniciales. Las funciones Hash garantizan la veracidad de los datos y su autenticidad. Los usos más destacados de las funciones Hash son los siguientes: Minería de criptomonedas, seguridad en las transacciones y generación de claves.

Figura 6. Algoritmo del Hash.



Nota: En esta imagen podemos observar cómo se está encriptando una información. La entrada es un archivo de texto plano, luego pasa por la función Hash, y por último lo convierte a un texto en Hash. *Tomado de: Editorial Team (2019). Hashing Algorithm. Fuente: https://networkencyclopedia.com/hashing-algorithm/*

Criptografía Simétrica

La criptografía simétrica se encarga del cifrado y/o descifrado requerido por dos entidades para encriptar o desencriptar un mensaje. Los algoritmos más conocidos son DES, 3DES, y AES. El principal reto del cifrado simétrico es la distribución y protección de las claves, lo que se combina con el cifrado asimétrico para resolver la transferencia segura de claves. Estos algoritmos se utilizan en aplicaciones de mensajería y almacenamiento en la nube para mejorar la seguridad de datos y la privacidad del usuario.

Criptografía de Clave Asimétrica

Los inventores de esta metodología fueron Merkle, Diffie y Hellman en 1976. Hoy en día es el método de cifrado más usado en internet. Este sistema requiere el uso de dos claves: una publica y otra privada. Según Gómez (2023) en su tesis, *Seguridad en el enrutamiento utilizando tecnología Blockchain, "*usando la clave pública de una persona, es posible cifrar un mensaje para que solo la persona con la correspondiente clave privada pueda descifrarlo y leerlo. Usando

una clave privada, se puede crear una firma digital para que cualquier persona con la clave pública correspondiente pueda verificar que el mensaje fue creado por el propietario de la clave privada y no se modificó desde entonces". Esto nos conceptualiza de forma general la importancia y el uso de cada una de las claves. La encriptación asimétrica genera pares de claves y sus longitudes con más largas que las generadas en la criptografía simétrica.

Proof of Work o Prueba de Trabajo

El *Proof of Work* es uno de los mecanismos de consenso que hay, y junto con el *Proof of Stake*, son los más usados. En este método hay participación de todos los mineros y se realiza para la validación de todas las transacciones. Las transacciones que ya han sido validadas son almacenadas en bloques.

Firmas Digitales

Las firmas digitales certifican documentos y garantizan su autoría. Algunos propósitos o características de la firma digital son:

- Autenticidad del autor.
- Integridad del documento.
- No repudio.

Árbol de Merkle

Tiene una estructura ramificada de árbol invertido, donde se expande desde los nodos base pasando a los nodos padre y al final llegar al nodo raíz. El nodo raíz es un identificador, los nodos base tienen asignado un hash y posterior a esto se concatenan en pares hasta terminar obteniendo un único hash principal. En la actualidad se usan con frecuencia para hacer más seguros los bloques de datos.

Contratos inteligentes en Blockchain

Los contratos inteligentes son simplemente programas almacenados en una cadena de bloques que se ejecutan cuando se cumplen condiciones predeterminadas se utilizan para automatizar la ejecución de un acuerdo para que todos los participantes puedan estar seguros de inmediato del resultado, sin la participación de ningún intermediario o pérdida de tiempo. (IBM, 2023).

Figura 7. Explicación de contrato inteligente.

NOTA: Esta figura explica el paso a paso de cómo se crea un contrato inteligente. *Tomado de: Rodríguez, N. (2018). recuperado el 13 de septiembre de 2024. Fuente: https://101blockchains.com/es/contratos-inteligentes/*

Estos contratos inteligentes ofrecen beneficios como lo son:

- Velocidad, eficiencia y precisión.
- Confianza y transparencia.
- Ahorros.
- Seguridad.

Uno de los aspectos más emocionantes de los Smart Contracts es su capacidad para crear seguridad jurídica en un mundo donde la confianza a menudo es un problema.

Los Smart Contracts son ampliamente utilizados en transacciones financieras, como préstamos, intercambio de activos digitales y pago de dividendos. Estos contratos automatizan la transferencia de fondos y garantizan que se realicen cuando se cumplen las condiciones adecuadas. Cuando ocurre un evento asegurado, el contrato puede verificar automáticamente la elegibilidad y emitir el pago correspondiente. La seguridad y la confianza son los pilares fundamentales que sostienen los Smart Contracts en el mundo de las inversiones, además de que cada transacción se verifica y registra en la Blockchain de manera transparente (Gracia, El método rico, 2023).

Teniendo en cuenta que la tecnología Blockchain es reciente y compleja, no pueden excluirse de fallos y vulnerabilidades a consecuencia de errores de programación, Identificadas éstas, resultan especialmente complicadas de parchear sin afectar al servicio debido a la arquitectura distribuida y la inmutabilidad de la cadena de bloques. Las vulnerabilidades se ven acentuadas por la multiplicidad de lenguajes de programación y protocolos, esto es, por la ausencia de estándares tecnológicos. Esta fragmentación ralentiza la curva de madurez de esta tecnología, reduce las posibilidades de detección de errores y de implantación de controles sobre

el código y dispersa la experiencia de los desarrolladores, sometidos a una presión constante para acortar los tiempos de entrega.

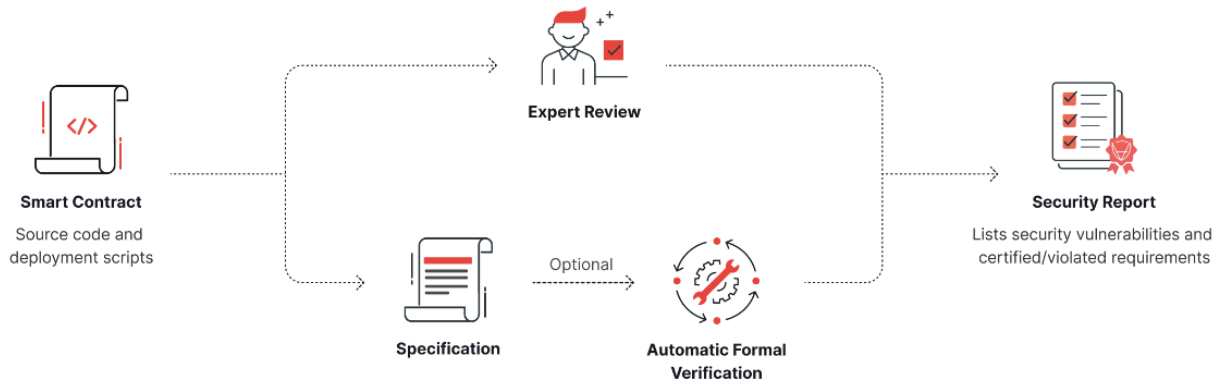
En relación con el empleo generalizado de Smart Contracts para llevar a cabo transacciones, éstos se ven expuestos a los errores y vulnerabilidades más probables en la medida en la que los Smart contracts son más complejos derivados de su codificación y de los de la plataforma de cadena de datos en la que se ejecutan (David Arroyo, Álvaro Rezola y Luis Hernández).

Blockchain Dapps

Las aplicaciones descentralizadas (Dapps), están diseñadas para existir en Internet sin que estén controladas por ninguna entidad en concreto, se ejecutan en una red P2P en lugar de en un único ordenador. Con una interfaz de usuario (frontend), que invoca contratos inteligentes (backend) alojados de forma descentralizada. Las Dapps impulsan distintas finalidades de la Blockchain, como plataformas DeFi, plataformas de criptopréstamos, mercados de NFT, préstamos P2P y otros (OpenMind. s/f).

La seguridad de la Blockchain que sostiene las DApps se deriva de su naturaleza distribuida. Estas a su vez utilizan criptografía avanzada, lo que garantiza la seguridad en las transacciones. Las transacciones en Dapps se registran de manera transparente y se almacenan en la Blockchain de forma pública. Esto permite que cualquier usuario audite y verifique las transacciones, lo que añade una capa adicional de seguridad. Algunos de los mecanismos de seguridad en DApps son las auditorias, donde plataformas famosas como Certik se encargan de auditar su código. CertiK es el auditor de contratos inteligentes y Blockchain recomendado por los principales exchanges como Binance, OKEx y Huobi (Certik.com. s/f).

Figura 8. Auditoria de un Smart Contract.



Nota: Aquí vemos cómo actúa la plataforma Certik en la auditoria de un contrato inteligente, el cual es revisado por un experto. *Tomado de: Certik (s/f). Smart Contract Audit. Consultado el 13 de septiembre del 2024. Fuente: https://www.certik.com/products/smart-contract-audit*

Conclusiones

Por medio de la investigación realizada fueron abordados lo conceptos básicos que componen la tecnología de Blockchain y fue posible determinar que es una tecnología que desde sus inicios ha sido innovadora, permite realizar transacciones de manera segura, eliminando la necesidad de intermediarios gracias a su estructura de bloques y descentralización. Es prácticamente imposible alterar o hackear los registros, lo que le da una gran ventaja en la trazabilidad y la transparencia de las transacciones, permitiendo así generar confianza y poder escalar cada día más en el mundo de la tecnología y los diferentes sectores.

El minucioso y fortalecido sistema de seguridad en Blockchain es uno de los pilares fundamentales que le permite ser tan confiable. Al usar registros distribuidos y encriptación avanzada, garantiza que las transacciones sean seguras, resistentes a manipulaciones, y permite que los usuarios tengan un nivel alto de confianza en los datos registrados; realmente su buen funcionamiento y su capacidad de mantener altos niveles de seguridad están haciendo que sus usuarios cada vez confíen más en esta tecnología.

Al usar la criptografía, que es la base de la seguridad en Blockchain, los algoritmos criptográficos y el algoritmo de hash, son los encargados de cifrar los datos, asegurando que tanto las nuevas transacciones, como la información previamente almacenada sean seguras y difíciles de hackear, garantizando la privacidad de los usuarios.

Aunque Blockchain es una tecnología segura, aún enfrenta riesgos importantes, como los relacionados con la escalabilidad y el manejo de grandes volúmenes de transacciones. Mas aún, sus sobresalientes resultados se han convertido en una fuente atractiva para entidades financieras, procesos de cadenas de suministros, procesos de votación electrónica, gestión de identidad, arte, derechos de autor, asignación de créditos, y también para muchas empresas de diferentes

sectores económicos, lo cual genera la necesidad de que Blockchain busque estrategias para mitigar estos riesgos y prevenir futuras fallas o interrupciones en su funcionalidad. Además, la falta de regulación y los ataques cibernéticos hacia aplicaciones descentralizadas también son desafíos que deben abordarse.

La seguridad transaccional en las DApps se apoya en los principios fundamentales de la tecnología Blockchain, como la descentralización, los contratos inteligentes y la criptografía avanzada. Sin embargo, la implementación segura de estos contratos y la continua revisión y auditoría del código son esenciales para garantizar que las Dapps funcionen de manera segura en el ecosistema Blockchain.

Referencias

Arroyo, D. Rezola, A y Hernández, L (s/f). Principales problemas de seguridad en los Smart Contracts de Ethereum. Recuperado el 12 de septiembre de2024. Fuente: https://www.ccn-cert.cni.es/es/pdf/documentos-publicos/xii-jornadas-stic-ccn-cert/3422-m22-02-smart-contracts-ethereum/file?format=html

Arteaga Caicedo, D. S. & Pantoja Eraso, L. M. (2022). Garantías de seguridad del sistema Blockchain para el sector financiero colombiano. [Trabajo de pregrado, Universidad CESMAG]. Repositorio Institucional de la Universidad CESMAG. http://repositorio.unicesmag.edu.co:8080/xmlui/handle/123456789/863.

Asixasantamaria. (2019). *Criptografía Simétrica.* Recuperado el 13 de septiembre del 2024. Fuente https://ciberseguridadasix.wordpress.com/2019/02/26/criptografia-simetrica/

Blockchain Federal Argentina (s/f). *Bloques y transacciones*. Recuperado el 13 de septiembre de 2024, de https://bfa.ar/blockchain/bloques-y-transacciones

Certik. Smart Contract Audit. Recuperado el 13 de septiembre de 2024. Fuente: https://www.certik.com/products/smart-contract-audit

Dai. Lu. Huang. (2024). Un sistema de control de acceso basado en Blockchain para cadenas de suministro de materiales peligrosos seguras y eficientes https://doi.org/10.3390/math12172702.

Gómez, M. A. (2023). Seguridad en el enrutamiento utilizando tecnología Blockchain. (Tesis de maestría. Universidad Nacional de la Plata). Disponible en: http://sedici.unlp.edu.ar/handle/10915/160784

Gracia, R. (2023). *Smart Contracts: ¿El Futuro de las Inversiones?* El Método RICO. https://elmetodorico.com/smart-contracts/

IBM. (2023). *What Is Blockchain Technology?* IBM; IBM. https://www.ibm.com/topics/blockchain.

Mithuyoshi, U. Sánchez, M. B. (2023). LA TECNOLOGÍA BLOCKCHAIN Y SU APLICACIÓN EN LA ADMINISTRACIÓN FINANCIERA. Revista FAECO sapiens, 6(2), 7-18. (fecha de Consulta 3 de septiembre de 2024). ISSN: 2644-3821. Disponible en: http://portal.amelica.org/ameli/journal/221/2214494001/

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. www.bitcoin.org.

Noriega C., Gustavo A., ¿Blockchain es más que criptomonedas?, presente y futuro (¿Is Blockchain More Than Cryptocurrencies? Present and Beyond) (enero 12, 2022). Apuntes Contables N°29, 2022, Disponible en: https://ssrn.com/abstract=4007440

Openmind. (Blockchain 4.0). Recuperado 13 de septiembre del 2024. Fuente: https://www.bbvaopenmind.com/tecnologia/mundo-digital/blockchain-4-0/

Retamal, C. D., Roig, J. B., & Tapia, J. L. M. (2017). La Blockchain: fundamentos, aplicaciones y relación con otras tecnologías disruptivas. *Economía industrial*, *405*, 33-40.

ROJAS, J. C. O. (2021). *Ciber seguridad de transacciones en sistemas de medición inteligente usando cadenas de bloques* (Tesis de Doctorado, INSTITUTO TECNOLÓGICO DE MORELIA). Disponible en: https://www.academia.edu/download/73403091/TesisFinalJCOR.pdf

Phemex. (2022). *La criptografía Blockchain: la columna vertebral de la seguridad Blockchain* - Phemex. Disponible en: https://phemex.com/es/academy/la-criptografia-blockchain

Rodríguez Gómez, J. L., Martínez Filgueira, X. M., & Peon Pose, D. O. (2020). *Bitcoin, un activo de inversión alternativo* [Tesis de Maestría. *Bitcoin, un activo de inversión alternativo*]. Disponible en: https://ruc.udc.es/dspace/bitstream/handle/2183/26065/RodriguezGomez_JoseLuis_TFM_2020.pdf?sequence=2&isAllowed=y

Rodríguez, N. (2018). *Contratos inteligentes: Guía definitiva para principiantes*. 101 Blockchains.com. Fuente: https://101blockchains.com/es/contratos-inteligentes/

Romero, R. Silva, A. Ramos, A. (2023). *Seguridad en transacciones electrónicas utilizando Blockchain*. Recuperado de: https://www.researchgate.net/profile/Alejandra-Silva-Trujillo/publication/373517249_Seguridad_en_transacciones_electronicas_utilizando_Blockchain/links/64efebc5f3514c57c43b42d2/Seguridad-en-transacciones-electronicas-utilizando-Blockchain.pdf

Seang, S., & Torre, D. (2018). Proof of Work and Proof of Stake consensus protocols: a blockchain application for local complementary currencies. *France: Universite Cote d'Azur-GREDEG-CNRS. Str*, *3*(4). Recuperado de: https://cointhinktank.com/upload/Proof%20of%20Work%20and%20Proof%20of%20Stake%20consensus%20protocols.pdf

Softtek (2018). El 70% del valor del Blockchain reside en la reducción de los costes. Recuperado el 13 de septiembre de 2024. Fuente: https://blog.softtek.com/es/el-70-del-valor-del-blockchain-reside-en-la-reduccion-de-los-costes

Tapscott, D. Tapscott, A. (2017). La revolución Blockchain. PAIDOS. Disponible en: https://www.academia.edu/35094257/DON_TAPSCOTT_LA_REVOLUCIO_N_BLOCKCHAIN