REVISTA
MULTIDISPLINARY JOURNAL



# Seguridad en las Transacciones del Protocolo Bitcoin, Ataques y Contramedidas.

## *Security in Bitcoin Protocol Transactions, Attacks and Countermeasures.*

Lic. Edwin Fernando Viteri Núñez [1*], Lic. Edilberto Antonio Llanes Cedeño [2]

1.* Doctor en Ciencias Administrativas, Escuela Superior Politécnica de Chimborazo, Riobamba, Ecuador. **Email:** eviteri@espoch.edu.ec **ORCID:** https://orcid.org/0000-0003-3029-775X

2. Doctor Dentro del Programa de Doctorado en Ingeniería Rural, Universidad Internacional SEK, Quito, Ecuador. **Email**: antonio.llanes@uisek.edu.ec **ORCID:** https://orcid.org/0000-0001-6739-7661

**Destinatario:** eviteri@espoch.edu.ec

**Recibido**: 08/Enero/2021 **Aceptado:** 12/Febrero/2021 **Publicado**: 31/Marzo/2021

**Como citar:** Viteri Núñez, E. F., & Llanes Cedeño, E. A. (2021). Seguridad en las Transacciones del Protocolo Bitcoin, Ataques y Contramedidas. E-IDEA 4.0 Revista Multidisciplinar 2(6), 10-20. https://doi.org/10.53734/mj.vol3.id151

**Resumen:** El presente artículo tiene el objetivo de analizar la seguridad en las transacciones del protocolo Bitcoin, sus ataques y contramedidas. En cuanto a la metodología se exhibe una investigación documental basada en la importancia de la seguridad en las transacciones del protocolo entre iguales (P2P) Bitcoin entre nodos de la red que conforman el ecosistema de monedas digitales. La revolución actual en cuanto al mercado de las criptomonedas ha impulsado el desarrollo de transacciones sin fronteras y sin intermediarios, lo que ha roto paradigmas en cuanto a libertad económica. Se estudia las características técnicas de las transacciones entre nodos P2P, se identifican los ataques en las transacciones y se describen las contramedidas que mitiguen posibles brechas de seguridad en el sistema. Como conclusión se menciona que, con la masificación actual del bitcoin es conveniente implementar mejoras en cuanto a los ajustes de la propagación de la información entre los nodos de la red, la gestión de las comunicaciones y los tiempos de propagación de la información entre ellos. Se pudo conocer que un adversario tiene por objetivo apropiarse de la red ofuscando a los nodos honestos para ganar tiempo de cómputo y energía para provechar estos recursos y apoderarse de las transacciones, teniendo un comportamiento de minado egoísta (selfishmining). Para evitar este comportamiento, es importante aplicar técnicas que mitiguen ataques de denegación de servicios que afecten a la red previniendo la entrega deliberada de bloques maliciosos en el sistema.

**Palabras clave:** Bitcoin, hash, transacción P2P, brecha de seguridad.

**Abstract:** This article aims to analyze the security of Bitcoin protocol transactions, its attacks and countermeasures. Regarding the methodology, a documentary research is exhibited based on the importance of security in Bitcoin peer-to-peer protocol (P2P) transactions between network nodes that make up the digital currency ecosystem. The current revolution in the cryptocurrency market has promoted the development of borderless transactions without intermediaries, which has broken paradigms in terms of economic freedom. The technical characteristics of the transactions between P2P nodes are studied, the attacks on the transactions are identified and the countermeasures that mitigate possible security breaches in the system are described. As a conclusion, it is mentioned that, with the current massification of bitcoin, it is convenient to implement improvements in terms of the adjustments of the propagation of information between the nodes of the network, the management of communications and the propagation times of the information between them. It was learned that an adversary has the objective of taking over the network obfuscating honest nodes to gain computing time and energy to take advantage of these resources and seize the transactions, having a selfishmining behavior. It is important to apply techniques that mitigate denial of service attacks that affect the network by preventing the deliberate delivery of malicious blocks to the system.

**Keywords:** Bitcoin, hash, transactions, P2P, security breach.

## INTRODUCCIÓN

Bitcoin es una colección de conceptos y tecnologías que forman los fundamentos del ecosistema de monedas digitales. Existe la unidad de moneda llamada bitcoin, se escribe así, con la "b" minúscula, y es empleada para almacenar y transmitir valor entre los participantes de una red bitcoin. Los tenedores de bitcoin se comunican entre sí (P2P) entre iguales, usando el stack del protocolo de comunicación Bitcoin, disponible como software libre, el cual puede ser ejecutado en una gran variedad de dispositivos computacionales, incluyendo laptops y teléfonos inteligentes, haciéndolo una tecnología de fácil acceso.

De acuerdo a (Ammous, 2018) es importante mencionar que la transferencia de bitcoin en una red, como moneda digital sirve como cualquier moneda de valor para comprar y vender bienes y servicios, enviar dinero a otras personas, en ese sentido, el bitcoin puede ser comprado, vendido e intercambiado por otras monedas en casas de cambios. Bitcoin se puede considerar una manera efectiva de dinero para el Internet porque es rápida, segura y sin restricciones de fronteras.

Por otro lado, se debe considerar que bitcoin es una moneda virtual, su circulación está basada en operaciones transaccionales enteramente digitales donde se transfiere valor desde un transmisor y un receptor. Los usuarios de bitcoin deben tener el control de sus propias claves o llaves que les permita firmar dichas transacciones para desbloquear el valor y gastarlo mediante la transferencia a un nuevo tenor.

Esto significa que por seguridad las claves deben estar almacenadas en una billetera digital, ya sea un dispositivo sólo para ello, en el teléfono o en el computador del usuario a las que pertenezcan las monedas digitales.

De allí pues la importancia de estudiar las características técnicas del protocolo Bitcoin que sustenta las transacciones entre iguales para el intercambio de monedas digitales, la identificación de las brechas de seguridad que pueden ser explotadas para vulnerar las transacciones y las técnicas que puedan mitigar estos ataques al sistema de intercambio de moneda digital entre pares.

Es pertinente mencionar algunas definiciones que son importantes comprender durante la lectura de la presente investigación para ello se muestran detalladamente en la Tabla 1

**Tabla 1**

*Definiciones importantes:*

| ASPECTO | DEFINICION |
|---|---|
| ***Bitcoin:*** | Nombre de una unidad monetaria virtual (la moneda), la red y el software para su funcionamiento. |
| ***Bloque:*** | Grupo de transacciones, marcados con un sello de tiempo y un hash del bloque anterior. La cabecera del bloque se le aplica un hash para producir una prueba de trabajo, así como para validar las transacciones. Los boques válidos son añadidos a la cadena de bloques principal a través de reglas de consenso en la red. |
| ***Cadena de bloques*** | Es la lista de bloques validados, cada uno de ellos enlaza a su predecesor hasta culminar con el bloque génesis (inicial). |
| ***Hash*** | Es una función matemática resumen o huella digital de alguna entrada binaria. |
| ***Minero*** | Nodo perteneciente a la red que consigue una prueba de trabajo válida para nuevos bloques, este proceso tiene un coste computacional que se consigue mediante la aplicación de hashing de manera concurrente. |
| ***Prueba de trabajo*** | Estructura de datos que requiere de coste computacional significativo. En bitcoin, los mineros deben conseguir una solución numérica al algoritmo SHA256 que cumpla los requerimientos de dificultad de la red. |
| ***SHA: Secure Hash Algorithm*** | Es una familia de funciones hash criptográficas publicadas por el Instituto Nacional de Estándares y Tecnología (NIST). |
| ***Transacción*** | Es una transferencia de bitcoin desde una dirección a otra. Una transacción es una estructura de datos firmada expresando una transferencia de valor. Las transacciones son transmitidas sobre la red de bitcoin, recolectada por mineros, y son incluidos en bloques, haciéndolos permanentes en la cadena de bloques o blockchain. |

**Fuente:** (Antonopoulos, 2014)

## MÉTODO

La redacción del artículo está sustentada como una investigación de tipo documental, se emplea una metodología que consiste en la revisión exhaustiva de documentación técnica, artículos científicos y libros digitales en la web, con fuentes actualizadas y ampliadas, mediante la técnica de arqueo de fuentes, revisión, cotejo e interpretación de datos para el desarrollo de los objetivos que sustentan la investigación, según la metodología de acuerdo a los autores especialistas (Hernández, 2014; Palella y Martins, 2015)

En este sentido, los objetivos de la investigación están contemplados en: Definir bitcoin como una moneda digital o virtual, ya abordado en la introducción de este artículo, identificar el protocolo de comunicación P2P Bitcoin, describir las características técnicas del stack del protocolo, enumerar los tipos de ataques existentes en las transacciones P2P,

conocer las técnicas de mitigación de estos ataques, concluir con el conocimiento de las buenas prácticas recientes para la fortificación de transacciones en el ecosistema de intercambio de monedas digitales.

## RESULTADOS

### Protocolo de comunicación entre iguales Bitcoin

Se define como un sistema distribuido entre pares, de manera tal que no existe un servidor central o punto de control. Bitcoin es creado a partir de un proceso computacional de alto costo, se conoce como minado, el cual consiste en la competición por encontrar la solución de un problema matemático mientras se procesan las transacciones de bitcoin (Nakamoto, 2008)

Debe considerarse que cualquier participante en la red bitcoin, que esté corriendo el stack completo del protocolo bitcoin, puede operar como un minero, usando la potencia de computo del procesador para verificar y registras las transacciones. Cada 10 minutos en promedio, un minero bitcoin es capaz de validar transacciones de 10 minutos anteriores y es recompensado con un nuevo bitcoin. En esencia, el minado de bitcoin descentraliza la emisión de moneda y reemplaza la figura de un banco central como intermediario para su validez y mantener confianza en las transacciones.

El protocolo Bitcoin está compuesto de algoritmos que regulan la función de minado a lo largo de la red. La dificultad de la tarea de procesamiento que el minero debe ejecutar es dinámicamente ajustada de manera que en promedio cada 10 minutos se pueda obtener ganancias independientemente de cuantos mineros haya en la red y de cuanto procesamiento esté presente.

Por otro lado, el protocolo Bitcoin hace una reducción a la mitad de la tasa de emisión de monedas digitales cada 4 años y limita el número total de bitcoin que serán creados a un número fijo preestablecido de hasta 21 millones de monedas. Con este proceso, se garantiza que el número de bitcoin circulante en toda la red se acercará a un número aproximado de 21 millones para el año 2140 (Antonopoulos, 2014)

Debido a la disminución de la tasa de emisión, sobre un largo periodo de tiempo, la moneda bitcoin es deflacionaria, además no puede ser “inflada” (es decir, que causa inflación) porque no se pueden imprimir nuevas monedas/billetes como lo hacen los bancos centrales.

*Propagación de la información a través de la red*

En una red Bitcoin se propaga la información vía DNS y por mensajes ADDR (Gervais et al. 2016). A continuación, se describe cada método de propagación:

- **DNS seeders:** es un servidor que responde a peticiones DNS provenientes de nodos bitcoin con una lista (no cifrada) de direcciones IP para nodos bitcoin. Los semilleros (seeders) obtienen estas direcciones verificando la red periódicamente. Estos semilleros son consultados cuando un nuevo nodo se une a la red bitcoin por primera vez, en este caso el nodo intenta conectarse con el semillero para obtener una lista de IPs activas, sino es exitoso, accede a un registro que contiene una lista de unas 600 direcciones IPs. El segundo caso ocurre cuando un nodo existente en la red se reinicia e intenta reconectar con sus nuevos pares, en la cual el semillero es consultado si han transcurrido 11 segundos desde que el nodo intentó reconectarse a la red y ha tenido menos de dos conexiones salientes (Gervais et al. 2016)

- **Mensajes ADDR:** Estos mensajes contienen hasta 1000 direcciones IP con sus respectivos sellos de tiempo, son utilizados para obtener información proveniente de los nodos en la red. Los nodos pueden aceptar mensajes ADDR sin haber sido solicitados. Estos mensajes son invocados cuando se establece una conexión saliente hacia un nodo, el par le responde con hasta 3 mensajes ADDR contentivos de hasta 1000 direcciones aleatorias seleccionadas de sus tablas. Los nodos envían mensajes ADDR a sus pares diariamente, es decir, un nodo envía su propia dirección IP a cada par, de esta manera, cuando un nodo recibe un mensaje ADDR con no más de 10 direcciones, este reenvía el mensaje ADDR de manera aleatoria a dos nodos de la red (Gervais et al. 2016)

*Ataque Eclipse*

Consiste en ofuscar al nodo victima para que no pueda ver a los nodos honestos de la cadena de bloques, por lo tanto, el nodo objetivo de ataque recibirá solamente conexiones entrantes y salientes de nodos maliciosos, esto con la intención de perpetuar transacciones de doble gasto (Heilman y Kendler, 2015)

De esta manera, el atacante puede poseer un gran número de direcciones IP a su disposición y controlar un conjunto de computadores que corran nodos en la red, por ejemplo, un botnet que pertenezca a un proveedor de servicios de Internet, y con ello se consigue que el atacante pueda dirigir una denegación de servicios que obligue al nodo objeto a restablecer el software cliente Bitcoin mediante una actualización de servicios.

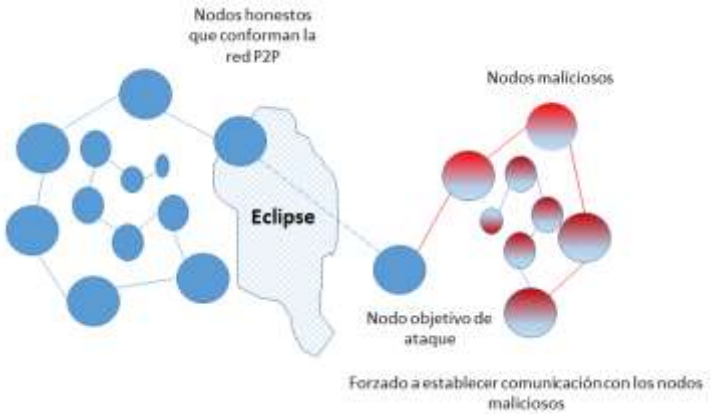
La actualización obliga a un reinicio del nodo, lo que causa que busque direcciones IP con sello de tiempo reciente y como el atacante ha inundado las tablas probadas con direcciones IP bajo su control y la tabla new con direcciones basura (inexistentes), tendrá la garantía de que la víctima efectivamente establezca conexión con un nodo bajo control del atacante.

En efecto, el algoritmo de ataque de eclipse cumple los siguientes pasos según indican (Heilman y Kendler, 2015):

> Explota la política de conectividad que usa la red Bitcoin entre sus pares P2P, aplicando una estrategia de llenado de direcciones IP basura a las tablas nuevas y de direcciones IP maliciosas en la tabla tratada; reiniciar al nodo objeto de ataque, aplicando denegación de servicio o alguna técnica que provoque el reinicio del sistema del sistema operativo o la memoria de los nodos; tomar el control de las conexiones entrantes y salientes del nodo víctima, considerando la probabilidad de éxito y la condición de selección aleatoria de las IP maliciosas provenientes de las tablas probadas.

Estos pasos anteriores causan la explotación de la vulnerabilidad en la política de conexiones y se logra eclipsar al nodo atacado, es decir, se monopoliza la conectividad del nodo con el resto de sus pares de la red y se puede observar en la Figura1

**Figura 1.**
*Representación Gráfica de un Ataque Eclipse*




**Fuente:** (Heilman y Kendler, 2015)

### *Ataque en las transacciones y poblado de nodos maliciosos en la red*

Una vez que la arquitectura de la red ha sido comprometida, con el reemplazo de direcciones IP válidas por maliciosas y comprometiendo la integridad de nodos honestos

que son forzados a conectarse a más nodos infestados, el atacante puede llegar a cumplir su cometido, el cual consiste en afectar las transacciones entre los nodos de la red (Gupta, 2018)

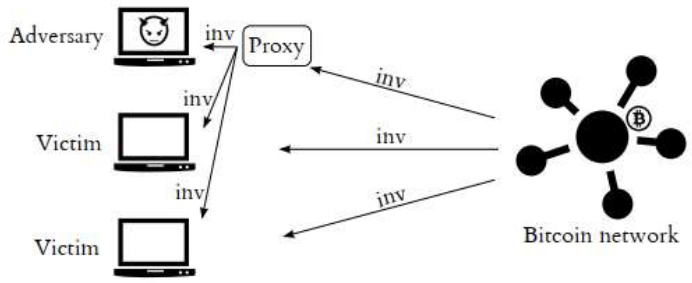
En este sentido, se atenta contra los tiempos de entrega de bloques y las transacciones. Para este caso el nodo malicioso busca la manera de restringir el flujo de información entre sus pares, usando un ataque de denegación de servicio, permitiéndole restringir la comunicación entre el nodo atacado y sus nodos vecinos honestos para la correcta propagación de la información (transacciones y hallazgo de nuevos bloques encontrados para agregarse a la cadena de bloques).

Para lograr lo anterior, el nodo malicioso explota la escalabilidad de la red Bitcoin, asegurándose de ser el primero en enviar el mensaje de anuncio de un objeto (bien sea una transacción o un bloque) al nodo atacado, con ello se asegura que el nodo atacado no volverá a hacer consulta a otro nodo vecino por la política de ahorro de ancho de banda y por lo tanto el nodo atacante se convertirá en el vecino más próximo del nodo atacado.

La condición anterior se satisface si el nodo malicioso implementa un proxy que se encargue de reenviar mensajes INV (inventario) sin la validación de objetos (bloques o transacciones). Por lo tanto, sin la validación respectiva, el nodo atacante gana tiempo comparado con el resto de los nodos honestos que usan tiempo y costo computacional para validar las transacciones, lo peor de este escenario es que estas peticiones inventario son masivas, lo que provoca la inundación o congestión de la red por parte del nodo atacante (Ver Figura 2)

**Figura 2.**

*Propagación de mensajes INV con un proxy por el nodo atacante*




**Fuente:** (Gupta, 2018)

En este sentido como indica Gupta (2018), cuando el nodo atacado acepta el mensaje INV, se procede a solicitar el mensaje de GETDATA, información de la transacción al nodo atacante, a lo cual éste no responderá y se consumirán en promedio 2 minutos de espera, por lo que el nodo atacado interrogará al siguiente nodo en la lista y tampoco recibirá

respuesta, por ser también un nodo atacante que ya ha poblado la tabla, esto obliga a un tiempo de espera con bucle obligado que se extienda a más de 20 minutos (Ver Figura 3)

De esta manera, el algoritmo de ataque en el retraso de las transacciones es la siguiente:

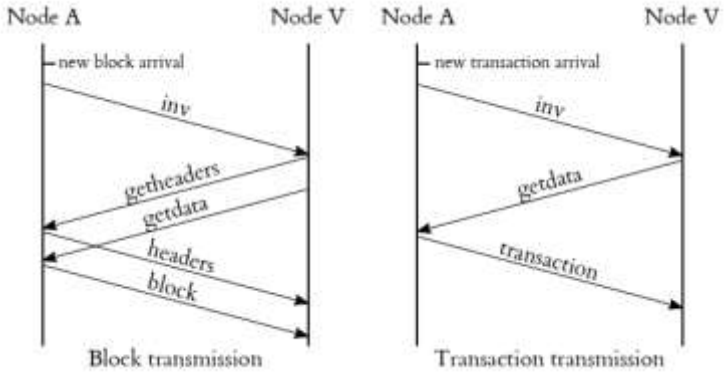
1. El nodo atacado acepta al menos una conexión proveniente del nodo atacante o malicioso.

2. El nodo malicioso debe ser capaz de mantener ocupadas los espacios de tiempo de conexión del nodo atacado.

3. El nodo atacante debe asegurarse de ser el primero en enviar mensajes de inventario INV de todos los bloques al nodo atacado, para tener el control total de esa porción de la red.

4. Reducir el número de conexiones al nodo atacado, de esta manera se asegura que no pueda recibir mensajes de nodos honestos y puede mantener la red ocupada en su dominio de ataque siendo satisfactoria la denegación de servicios (Gupta, 2018)

**Figura 3.**
Propagación de mensajes entre el nodo atacante y el nodo victima




**Fuente:** (Gupta, 2018)

Los resultados de la presente investigación relacionada al estudio de la arquitectura de la red bitcoin y los tipos de ataque a los que se pudiera someter, demuestra con el siguiente apartado de contramedidas a un conjunto de técnicas de mitigación que limiten o impidan el daño causado en las transacciones de la red Bitcoin.

*Contramedidas:*

Algunas medidas para mitigar o contrarrestar la propagación del ataque por parte de nodos maliciosos que puedan afectar la red (Gervais et al. 2016) se describe lo dispuesto en la Tabla 2

**Tabla 2.**
Medidas para mitigar la propagación del ataque por parte de nodos maliciosos

| MEDIDAS | DESCRIPCIÓN |
|---|---|
| *Implementar tiempos de espera dinámicos* | Ya que hay nodos que son más lentos que otros para descargar los bloques, debido a limitaciones de ancho de banda, entonces es necesario implementar tiempos de espera que sean adaptables a la heterogeneidad de la red. Para ello se sugiere la inclusión del tamaño del mensaje al momento de anunciarse en la red, lo cual permitiría a cada nodo estimar dinámicamente el tiempo de expiración de acuerdo a sus recursos y el tamaño del objeto.<br>De esta manera, cuando se esté enviando un mensaje de anuncio de bloque, el minero incluye el tamaño del bloque dentro de la cabecera del mismo, con esta política, los nodos receptores pueden conocer el tamaño del bloque y de manera apropiada poder estimar dinámicamente el tiempo de espera. Con esta contramedida, un nodo malicioso se le haría más difícil poder abusar con el retraso de entrega de bloques. |
| *Mantener actualizados los anuncios de bloques* | Se sugiere dejar de utilizar mensajes de solicitud de inventario INV para anunciar bloques y solamente usar las cabeceras antes de la retransmisión de los bloques. Con esto, el nodo receptor verificará la validez del PoW y aprende acerca de cualquier bloque nuevo que ha sido descubierto en la red. Al mismo tiempo, como el tamaño de la cabecera de un bloque es de 80 bytes, comparado con un mensaje *inv* que ocupa 36 bytes, tampoco sería un problema una saturación en la red por esta modificación. |
| *Mantener registro del anuncio de bloques* | Tal como ocurre en el anuncio de las transacciones, también debe mantenerse un registro en los nodos de la red respecto al anuncio en las cabeceras de los bloques. Esto permite a un nodo solicitar bloques de aquellos pares que anuncian la cadena más larga. Adicionalmente, permite a un nodo solicitar el anuncio de un bloque desde un par elegido aleatoriamente, en caso de que haya retardo en la entrega del bloque por parte de un nodo. |
| *Gestión en el anuncio de transacciones* | La transacción entre los nodos de la cadena de bloques es solicitada por aquellos nodos que primero han anunciado la operación en la red. Si por alguna razón, el nodo no responde y expira el tiempo de anuncio, entonces es consultado el siguiente nodo en la cola FIFO – First In FirstOut. Esto da una ventaja considerable al nodo atacante en dilatar el tiempo de espera por un nodo para informarse de las transacciones en la red. |

**Fuente:** (Gervais et al. 2016)

## CONCLUSIONES

Se llega a concluir que, con la masificación actual del bitcoin es conveniente implementar mejoras en cuanto a los ajustes de la propagación de la información entre los nodos de la red, la gestión de las comunicaciones y los tiempos de propagación de la información entre ellos.

Se pudo conocer que un adversario tiene por objetivo apropiarse de la red ofuscando a los nodos honestos para ganar tiempo de cómputo y energía para provechar estos recursos y apoderarse de las transacciones, teniendo un comportamiento de minado egoísta (selfishmining).

Para evitar este comportamiento, es importante aplicar técnicas que mitiguen ataques de denegación de servicios que afecten a la red previniendo la entrega deliberada de bloques maliciosos en el sistema.

## REFERENCIAS BIBLIOGRÁFICAS

Ammous, S. (2018). The Bitcoin Standard: The Decentralized Alternative to Central Banking. Grupo Editorial John Wiley & Sons.

Antonopoulos, A. (2014). Mastering Bitcoin: Unlocking Digital Cryptocurrencies. Grupo Editorial O'Reily Media.

Gervais, A., Ritzdorf, H., Karame, G., & Capkun, S. (18 de Septiembre de 2016). Tampering with the Delivery of Blocks and Transactions in Bitcoin. NEC Laboratories Europe, Germany. 22nd ACM SIGSAC Conference on computer and communications security , 692-705.

Gupta, R. (2018). Hands-On Cyber security with Blockchain. Implement DDos protection, PKI-based identity, 2FA and DNS security using Blockchain. Grupo editorial Packt Publishing Ltd.

Heilman, E., & Kendler, A. (2015). Eclipse AttacksonBitcoin's Peer-to-Peer Network. 24th USENIX Securiity Symposium .

Hernández. (2014). Metodología de la Investigación. Grupo editorial McGrawHill.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Recuperado el 24 de Septiembre de 2021, de https://bitcoin.org/bitcoin.pdf.

Palella, S., & Martins, F. (2015). Metodología de la investigación cuantitativa. 3ra Edición. Recuperado el 24 de Septiembre de 2021, de https://es.calameo.com/read/000628576f51732890350