



**UNIVERSIDAD TÉCNICA DE BABAHOYO**  
**FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA**

**PROCESO DE TITULACIÓN**

**ABRIL 2024 - AGOSTO 2024**

**EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA**

**PRUEBA PRACTICA**

**PREVIO A LA OBTENCIÓN DEL TÍTULO DE:**  
**INGENIERA EN SISTEMAS DE INFORMACIÓN**

**TEMA:**

**ALGORITMOS DE CLOUSTERING PARA INVESTIGACIONES FORENSES DE  
TRANSACCIONES DE BLOCKCHAIN.**

**ESTUDIANTE:**

**PACHECO GALARRAGA ANGIE ALEXANDRA**

**TUTOR:**

**ING. RAUL RAMOS**

**AÑO 2024**

## ÍNDICE

RESUMEN .....	3
INTRODUCCIÓN.....	4
PLANTEAMIENTO DEL PROBLEMA .....	5
JUSTIFICACIÓN.....	8
OBJETIVOS DEL ESTUDIO .....	10
Objetivo General.....	10
Objetivos Específicos .....	10
LÍNEAS DE INVESTIGACIÓN .....	11
MARCO CONCEPTUAL .....	12
MARCO METODOLÓGICO .....	27
RESULTADOS .....	29
DISCUSIÓN DE RESULTADOS .....	33
CONCLUSIONES.....	34
RECOMENDACIONES .....	35
REFERENCIAS .....	36
ANEXOS.....	40

## RESUMEN

Los actos ilícitos hoy en día están tomando fuerza diariamente, en donde toman a las nuevas innovaciones tecnológicas como un beneficio para los delincuentes, como lo es la tecnología blockchain, que se basa en ser una red transparente en donde se pueden realizar una variedad de transacciones en milisegundos, esta tecnología es utilizada comúnmente en plataformas de bitcoin, Ethereum etc. Estas plataformas utilizan las criptomonedas que es una forma de moneda digital, realizando un sinnúmero de procesos como compras ventas o movimiento de dinero.

A pesar de ser una tecnología innovadora, esta, intensiva las estafas, fraudes, el lavado de dinero e incluso las ventas de drogas o la trata de personas, ya que los delincuentes hacen uso de estas plataformas para realizar movimientos, teniendo la opción de hacerlas de manera anónima y tienen la estrategia de utilizar varias plataformas y realizar movimientos en varias transacciones para dificultar ser rastreados, por ello, el estudio de los algoritmos clustering nace como una estrategia para ayudar a los analistas forenses a rastrear y realizar un análisis profundo en la red blockchain para así identificar patrones y agilizar el proceso de búsqueda de los actores delictivos, teniendo como objetivo principal “Evaluar la efectividad de los algoritmos cloustering para detectar transacciones blockchain, para actividades ilícitas”, para cumplir con el objetivo se hizo necesario integrar la investigación explorativa y comparativa con los métodos cualitativo y bibliográficos, también se utilizaron técnicas como la encuesta y la observación.

**Palabras clave:** Blockchain, Transacciones, Datos, VirtualBox, Criptomonedas, Análisis Forense, Python.

## INTRODUCCIÓN

Hoy en día una fuente que ah tomada fuerza al pasar el tiempo, es el uso de la criptomoneda, que se basa en la tenencia de dinero virtual, en diversas cuentas, partiendo de una red blockchain, donde engloba todos estos procesos, permitiendo realizar un sin número de transacciones desde la comodidad de sus hogares y oficina, pero así, como es una herramienta que facilita la vida de las personas, el mal uso de esta, provoca estafas y diversos actos delictivos por delincuentes.

Las transacciones blockchain tiene similitud a un libro de contabilidad, con accesos compartido e inmutables que ayuda a registrar procesos de transacciones y por ende el seguimiento de los activos en una red empresarial, en donde, los investigadores forenses toman como referencia esta tecnología para rastrear este tipo de transacciones.

Existen diversos problemas enlazados con las transacciones blockchain, en un análisis forense, ya que, los delincuentes realizan múltiples solicitudes de diferentes cuentas dificultando el rastreo de esas transacciones, pasando fronteras y ocultando los procesos y estrategias delictivas para ser evitado.

Los algoritmos cloustering nace como un énfasis de solución y ayuda para el rastreo de transacciones anormales en una red blockchain para que las investigaciones forenses sean más rápidas y concisas. La inyección de estos algoritmos en una red blockchain, rastrea profundamente la red, obteniendo resultados hasta de acciones ocultas de la misma.

Por ello, el propósito de este caso de estudio, es evaluar la efectividad de los algoritmos cloustering, como un medio de solución para las investigaciones forenses, para detectar transacciones blockchain, en actividades ilícitas.

## **PLANTEAMIENTO DEL PROBLEMA**

La diversidad y la dispersión de la información digital continúa creciendo exponencialmente en donde los entornos legales y regulatorios se vuelven cada vez más desafiantes día a día, a partir del siglo XXI la tecnología ha innovado y transformado muchos aspectos de la vida cotidiana e incluso diversos negocios, mejorando su estabilidad y economía. Entre las aportaciones de la tecnología está, la adopción de Blockchain en donde es popularizada por el surgimiento de las Criptomonedas, ofreciendo sistemas más descentralizados, brindando transparencia y seguridad en las transacciones.

A medida de que la tecnología evoluciona, los datos y registros también van en aumento, existiendo muchas maneras de obtener información por medio de formatos y capacidades de almacenamiento, cada día, las transacciones en blockchain son más comunes y varían en diversos casos, con su aumento se hace más difícil rastrear y analizar sus flujos, por ello, uno de los principales problemas se basa en el déficit para identificar o rastrear a los actores involucrados directamente en actividades delictivas debido al alto porcentaje de anonimato y seudonimito asociado con direcciones de billetera en blockchain. La falta de transparencia de estas transacciones en cantidades elevadas dificulta a las autoridades seguir el flujo de los fondos y por ende comprender la red de las transacciones relacionadas con estas actividades ilegales.

Existe una variedad de actividades ilícitas que son utilizadas por medio de esta herramienta tecnológica, entre las más comunes, está el lavado de dinero, los delincuentes, utilizan transacciones por medio de blockchain convirtiendo el dinero fiat en criptomonedas, para así realizar una variedad de transacciones que tienen como propósito ocultar el origen de los fondos monetarios.

También esta la financiación del terrorismo en Ecuador, Colombia y en una variedad de países, en donde utilizan las criptomonedas, para que las personas involucradas en esta red

ilegal, pueden recibir dinero como una forma de donación, permitiéndoles mover fondos de manera local e internacionalmente sin tener algún contacto con entidades bancarias legales, por otro lado, están los fraudes y estafas por medio de los esquemas Ponzi y ICOs en donde se basan en atraer inversiones a estas plataformas con el dinero virtual o criptomoneda para luego desaparecer los fondos de los inversores y no poder tener ningún contacto alguno, estas son más conocidas como paginas fantasma.

El tráfico de drogas en mercados en línea como la página de darknet hace uso de estas monedas y con ello las demandas de rescate de ransomware y entre las más usuales de las activadas ilícitas se involucra la explotación sexual, en donde usan criptomonedas para vender y comprar, incentivando al tráfico humano y manteniendo un anonimato en cada transacción hechas en estas plataformas.

Esto representa un desafío para las autoridades y la sociedad en general ya que cualquier persona puede ser víctima de alguno de estos casos y para dar con el paradero de los autores es necesario hacer un seguimiento de cada transacción e identificar patrones que ayuden a socorrer o detener estas actividades, para la sociedad, esto representa un acto de inseguridad y desconfianza con las nuevas innovaciones tecnológicas en general y más con tecnologías financieras, basándose en convertir el dinero físico a virtual, en donde puede afectar negativamente la economía de la sociedad y autoridades.

Cabe mencionar, que las transacciones pueden pasar fronteras internacionales y aumentar cada vez más, la dificultad de rastrearlas por parte de autoridades nacionales, investigadores y personal profesional y especializado en el análisis forense, esto ocurre por medio de la evolución constante de las estrategias delictivas para no dejar rastros de los delitos, entonces se hace necesario abordar temas relacionados con los algoritmos clustering para investigaciones forenses en redes blockchain, encargados de agrupar datos en funciones similares teniendo patrones comunes, ofreciendo un enfoque más específico para rastrear e identificar actividades

que pueden parecer sospechosas en cantidades elevadas de transacciones.

El volumen y la gran cantidad de estos datos, hacen más complejo el uso de rastreadores de manera humana, generando más falencias e hitos en su detección, ya que la tecnología blockchain actúa de manera continua generando grandes cantidades de datos los cuales, los investigadores deben analizar, para dificultar su rastreo, los delincuentes realizan miles de transacciones de pequeño tamaño como distracción, con ello, la difícil identificación de patrones de esas transacciones y el análisis de estas informaciones echa de manera manual es ineficiente, resultando en una solución poco favorable para su reconocimiento, debido a la escala de transacciones, apunta directamente a implementar y utilizar herramientas automatizadas que faciliten estos aspectos al ser humano para ser más eficientes, como lo son los algoritmos forenses.

Pero, existen algoritmos estándar que no identifican de manera efectiva todos los procesos de transacciones en blockchain, en donde no identifican los patrones ocultos entre las transacciones, siendo producidas por la variabilidad y la ofuscación que los delincuentes crean para ser irrastreadable.

Los delincuentes utilizan diferentes criptomonedas por medio de la herramienta blockchain interoperando entre diferentes plataformas para transferir los fondos, haciendo que se fragmente aún más los datos, en donde los algoritmos comunes no pueden interpretar o manejar las fragmentaciones, ocasionando que la investigación se ralentice y tenga un menor porcentaje de detección de actividades ilícitas, por ello, se hace el estudio de los algoritmos cloustering, que se basa en ser una herramienta eficiente para el análisis de grandes cantidades de datos permitiendo su agrupación en un conjunto de objetos.

## JUSTIFICACIÓN

A medida que el tiempo pasa y la evolución constante de la tecnología aumenta día a día, la adopción de las criptomonedas está en crecimiento constante, según (Jenkinson, 2024) , el número de usuarios de criptomonedas en todo el mundo en el año 2023 supero los 580 millones en comparación con el año 2019 que tubo 100 millones de usuarios. Esto representan un aumento critico en la adopción de la moneda virtual, en donde las inversiones en criptomonedas han crecido exponencialmente en diversas empresas como Tesla y MicroStrategy, en donde han invertido millones de dólares en la plataforma digitales como Bitcoin.

Las criptomonedas hacen una dupla con la tecnología Blockchain, revolucionando de manera idónea todo el sistema financiero a nivel mundial, impartiendo un sinnúmero de beneficios a todas las personas que haces uso de ella, como lo son las transacciones seguras desde la comodidad de sus hogares, siendo muy rápidas, de fácil uso y al mismo tiempo siendo transparentes en cada una de las transacciones por medio de una tecnología llamada Blockchain.

Las plataformas como BitPay ha alcanzado más de 1mil millones de transacciones exitosas y seguras en el año 2022, esto revela que el uso de las criptomonedas facilita las transacciones de forma segura y eficiente, ya que esta, es una plataforma de pagos que trabaja a nivel global que está disponible en más de 150 países a nivel nacional, permitiendo el intercambio de criptomonedas (Partz, 2022).

A pesar de traer solución a la vida de las personas sin necesidad de la presencia física, está, está propensa a facilitar el lavado de dinero y estafas por personas que hacen uso inadecuado de los avances tecnológicos. Para los delincuentes, es una forma fácil y favorable manejar el dinero de manera virtual, a pesar que los bancos tengan restricciones y se mantengan al tanto de las transacciones de sus usuarios, el uso de esta plataformas que utilizan criptomonedas, tienen la opción de hacer transacciones de manera anónima en muchas ocasiones, ya que el dinero no pasa necesariamente por bancos legales y se las ingenian para pasar desapercibidos,



esto lo hacen utilizando múltiples transacciones en diferentes sistemas financieros, haciendo más complejo su rastreo.

Binh Thanh Le de Brockton, fue uno de los primeros en poner en marcha un negocio ilícito de drogas, utilizando la plataforma de Bitcoin, en donde le generaba más de 59 millones de Bitcoin, al ser descubierto, las autoridades le incautaron aproximadamente 2,3 millones de dólares en esta plataforma y más 114 mil en efectivo, el mercado de Darknet que manejaba, le permitía realizar transacciones anónimas y por ende en pequeñas partes para no ser descubierto (Chipolina, 2022).

Por otro lado (Newar, 2022), Publico que desde el 10 de febrero las, actividades de ransomware exige pagos a organizaciones utilizando criptomoneda, este malware desactiva los softwares de seguridad tras un primer acceso, en donde, este uso, ha crecido en el 2021 y afirma que supero y seguirá superará valores del 2020 con 692 millones de ese año.

El análisis forense de transacciones blockchain, se basa en analizar la red de las transacciones y se destaca por detectar y prevenir las actividades ilegales, pero el uso de herramientas o algoritmos cotidianas como; Chainalysis, Elliptic, CIPHERTRACE o Crystal Blockchain, a pesar de que cumplen sus funciones al analizar datos de una red blockchain, estas generan una falencias, no hacen un análisis profundo y demora en detectarlas, ralentizando el proceso de los forenses, siendo poco eficientes.

Por ello, se hace necesario el estudio de los algoritmos clustering de manera avanzada, encargándose de facilitar la agrupación y el análisis de grandes cantidades de transacciones, ayudando a identificar los patrones y con ello las relaciones ocultas que incitan a ser sospechosos e ilegales. Por otro lado, estos algoritmos tienen la ventaja de ser adaptativos, es decir se adaptan con facilidad a nuevos patrones y datos, siendo una ventaja destacada en un entorno donde las estrategias delictivas van en aumento constante.

## **OBJETIVOS DEL ESTUDIO**

### **Objetivo General**

- Evaluar la efectividad de los algoritmos clustering para detectar transacciones blockchain, para actividades ilícitas.

### **Objetivos Específicos**

- Analizar los algoritmos clustering en la detección de actividades ilícitas en transacciones blockchain.
- Investigar hallazgos de prácticas con los algoritmos clustering para identificar técnicas más utilizadas.
- Examinar las características y las limitaciones que tienen cada uno de los algoritmos clustering.

## LÍNEAS DE INVESTIGACIÓN

La facultad de administración finanzas e informática aprobó el tema: Algoritmos de cloustering para investigaciones forenses en transacciones de blockchain, perteneciente a la carrera de Sistemas de información rediseñada de la Universidad Técnica de Babahoyo, en donde se relaciona y hace énfasis a las líneas y sublínea de investigación:

- **Línea de investigación**

Sistemas de información y comunicación emprendimiento e innovación.

- **Sublínea de investigación**

Redes y tecnologías inteligentes de software y hardware.

Este tema se relaciona con la línea de investigación de sistemas de información y comunicación emprendimiento e innovación, ya que el desarrollo de este estudio busca analizar los algoritmos cloustering que pueden ayudar a perfeccionar sistemas de análisis forense avanzados para identificar y rastrear actividades ilícitas en los sistemas, ahorrando tiempo y facilitando el análisis de forma humana o manual, siendo una alternativa novedosa e innovadora en el área de la tecnología y manejo de información de las transacciones.

También tiene una estrecha relación con la sublínea de investigación de redes y tecnologías inteligentes de software y hardware, haciendo mención y relación con la estructura de la red blockchain, en donde la evaluación de los algoritmos cloustering implica el uso de redes de datos y la integración de software y hardware en análisis forenses.

## MARCO CONCEPTUAL

La innovación y la tecnología van estrechamente relacionadas, encargándose de simplificar procesos manuales humanos en la detección de irregularidades en los sistemas empresariales y financieros, manejados por la criptomoneda.

Al pasar los meses y años, este tipo de innovación tecnológica se va actualizando constantemente, en dónde especialistas en análisis de requerimientos, desarrolladores de software, gestión de riesgos, analista de redes o telecomunicaciones, son los encargados de desarrollar soluciones innovadoras con el fin de agilizar y automatizar procesos que le toman tiempo a al ser humano desarrollarlas de forma manual, éstas soluciones deben ser efectivas y rápidas, ayudando así, a mantener informado al personal o gerencia de la fluidez de su empresa o negocio, con ello facilita la detección de anomalías de forma rápida, para la toma de decisiones.

Como dice (Canedo , 2019, pág. 6) la importancia de los sistemas de información toma mayor fuerza en una sociedad que está enmarcada en una era digital, evolucionada en la tecnología y el conocimiento impulsada por la revolución de la tecnología, proporcionando a las empresas optimizar procesos, ayudar a la toma de decisiones e identificar anomalías.

### **¿Qué es VirtualBox?**

Esta es una herramienta de código abierto, utilizada comúnmente para realizar proyectos en máquinas virtuales, catalogada por la creación e instalación de sistemas operativos alternos, se la conoce como un software de virtualización multiplataforma de código abierto mas popular del mundo por los desarrolladores.

En esta plataforma se pueden realizar diversas emulaciones de múltiples sistemas, realizar configuraciones como si se tuviera un equipo alternó en una misma maquina física, pero cabe mencionar que uno de los requerimientos para tener N cantidad de maquinas virtuales, es tener un equipo físico potente, con un mínimo de 8G de RAM y 250 de disco duro, ya que al levantar

una maquina virtual, este toma recursos de la maquina física para que funciones eficazmente, por ello si se necesita levantar más de una máquina, se debe tener una buena maquina física.

### **Python**

Este es un lenguaje de programación muy utilizado en la web, comúnmente en desarrollo de software, ciencia de datos y en machine learning, este software de programación es muy eficiente y fácil de aprender para muchos programadores e incluso en servidores web, siendo muy eficiente y se adapta o se puede ejecutar en múltiples plataformas diferentes.

Entre los beneficios de este software esta que cuenta con una variedad de bibliotecas y librerías que son útiles para proyectos pequeños y grandes, estas bibliotecas son estándar y pueden ser reutilizables en los proyectos para casi cualquier tarea, y es compatible con cualquier otro programa en combinación.

### **Librería Scikit-Learn**

Esta librería esta basada en el aprendizaje automático siendo popular en el análisis forense en las redes blockchain ya que es extremadamente popular y contiene una amplia comunidad al ser utilizada en Python.

Esta, contiene una amplia gama de algoritmos a utilizar o implementar, y con ello, diversas herramientas que complementan su uso es proyectos Python.

### **Librería Pandas**

Pandas está diseñada especialmente para la manipulación y el análisis de datos en lenguaje Python y con ellos el análisis de datos en este mismo lenguaje, siendo un software potente y , flexible.

### **GEPHI**

Según (Fernández, 2023, pág. 3) , Gaphi radica en ser una herramienta encargada de la virtualización de redes y análisis de datos, permitiendo la exploración y la comprensión de la similitud de datos, este software permite crear gráficos y también identificar patrones,

tendencias y similitudes clave entre una cantidad de datos.

Esta herramienta es útil en este estudio, ya que permite a los analistas forenses ajustar interactivamente los parámetros de los algoritmos de clustering, con el fin de mejorar la precisión en la identificación de los patrones y las anomalías en las transacciones realizadas en una red blockchain, este, ayuda a interpretar de mejor manera los resultados a través de la virtualización relacionada con los algoritmos clustering.

### ¿Qué es la criptomoneda?

La criptomoneda es una tecnología actual, radica en el uso de activos virtualizados descentralizados, que no están controlados ni respaldados por alguna entidad bancaria central, en donde se pueden hacer transacciones con libertad y desde cualquier lugar, su control parte normalmente de una blockchain que es básicamente una cadena de bloques.

Según (Carrera López et al, 2020) las transacciones con criptomonedas son manejadas por los propios desarrolladores y usuarios registrados en estas aplicaciones, evitando el paso físico a entidades bancarias, siendo cada vez más común su uso en establecimientos comerciales y en Latinoamérica cada vez se suma más a aceptar pagos por este, medio.

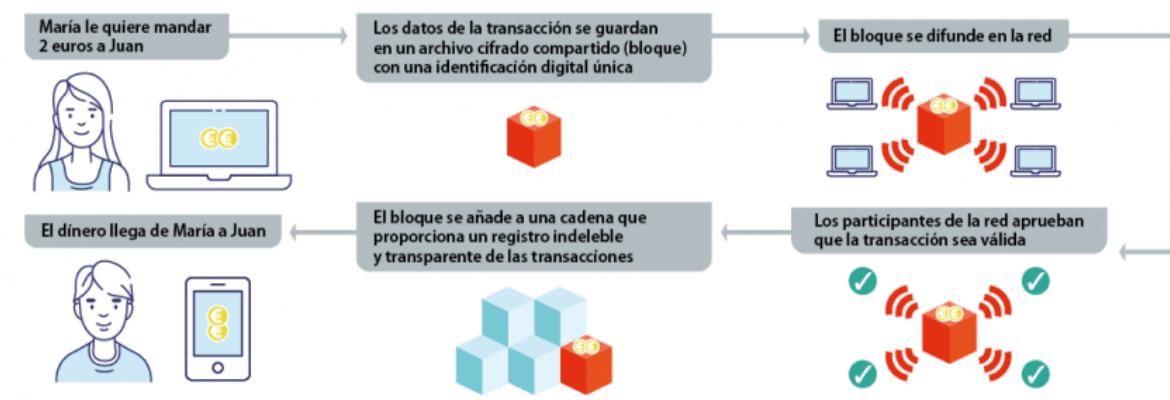


Ilustración 1: Transacción de criptomoneda en una Blockchain (García Arenas, 2019)

En el caso de la criptomoneda, es muy común que a nivel global las personas hagan uso de esta herramienta o forma de billetera virtualizada, manteniendo su dinero o finanzas en las llamadas criptomonedas, tomada como una opción ventajosa para evitar el efectivo y por ende

la facilidad que otorga de realizar pagos e incluso compras en línea desde la comodidad de sus hogares, pero como toda innovación tecnológica tiene sus desventajas.

### ¿Que son Esquemas Ponzi y ICOs?

Esta es una forma de estafa que ah revolucionado el mundo contantemente, son mas conocidas como tratos piramidales, en donde consiste en convencer y persuadir a la victima para que invierta cierta cantidad de dinero en algún tipo de plataforma eh incluso lo hacen de manera presencial o utilizando redes, pero es más común que lo hagan de manera virtual, los involucrados en este negocio o forma de estafa, se benefician de los nuevos aportadores ganando monedas, pero a medida que este esquema Ponzi los inversionistas mayores, son los mas beneficiados en esta red.

### Esquema Ponzi

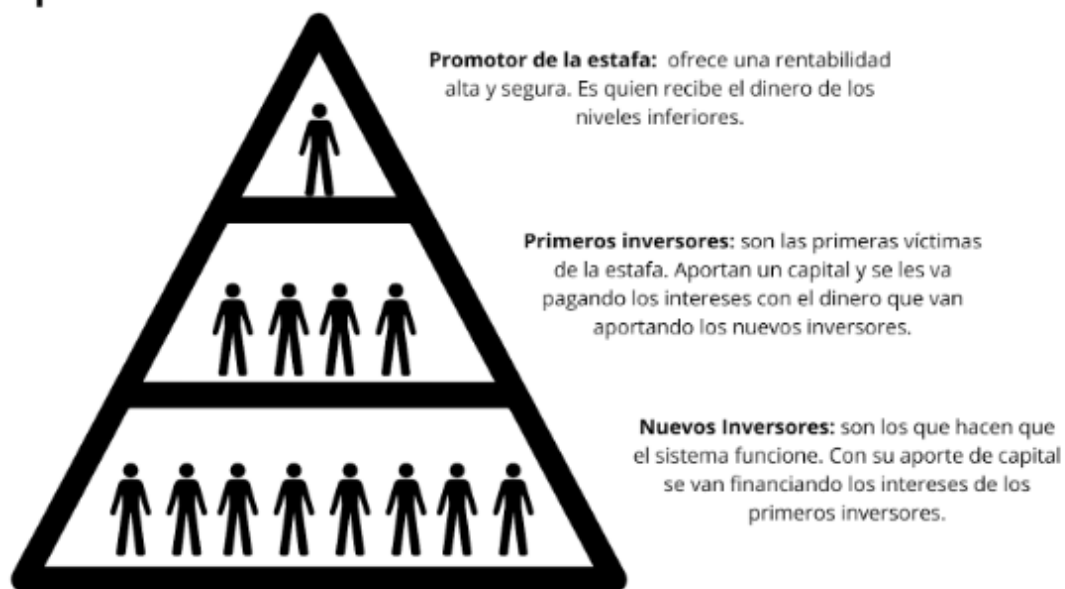


Ilustración 2,: Función del esquema Ponzi Fuente: (Pérez, 2024)

Para (Cargo Suarez, 2022, pág. 12) en la utilización de criptomonedas, estas siguen el mismo modelo o reglas de estafa en estas plataformas, pero lo hacen de manera digital, utilizando un activo para incentivar la inversión y que el proyecto sea mas real y creíble para las víctimas, siendo una de las más mencionadas que es el OneCoin que ha llegado a estafar millones de

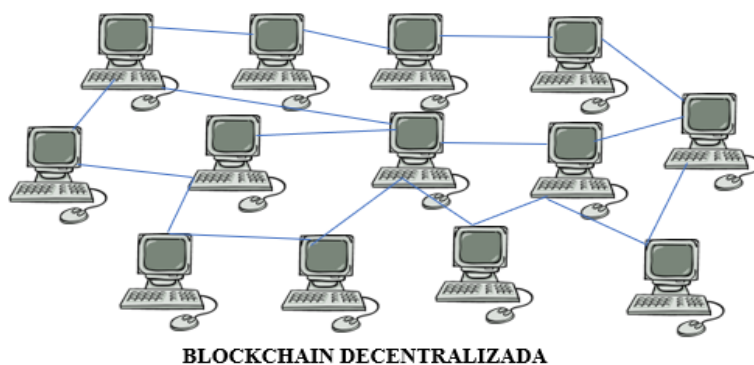
personas por medio de las criptomonedas y por ende se convierten en dólares.

Por otro lado, los ICOs es básicamente una forma de recaudación de criptomoneda por medio de productos o servicios, siendo muy similar a las ofertas publicitarias, pero estas monedas también son emitidas como inversión de compras ventas y estafas y pueden tener valor para pagar servicios o software,

### ¿Qué es Blockchain?

Blockchain es una tecnología que ha venido tomando fuerza al pasar los años, siendo una forma segura de realizar procesos. Se basa en una red de gran tamaño que es capaz de realizar múltiples procesos o transacciones al mismo tiempo, teniendo protocolos estrictos y una similitud en cada transacción, siendo imposible la alteración de códigos o patrones de cada una de las transacciones a nivel de red.

### Funcionamiento de blockchain



*Ilustración 3: Función de una Blockchain descentralizada. Fuente; Propia*

Básicamente, esta ilustración, representa el funcionamiento descentralizado de una red blockchain, basándose en almacenar información en toda una cadena de bloques, en donde, cada bloque de esta red, contendrá un conjunto de transacciones verificadas y a la vez estarán conectadas al bloque anterior, conteniendo un hash único en todos los bloques, distribuyéndose en múltiples nodos interconectados, siendo innecesaria que se guarde en una autoridad central.

Para (Perez Medina, 2020, pág. 1)Blockchain es una tecnología utilizada para el almacenamiento de datos que crece de forma acelerada, esta es la tecnología mayoritariamente utilizada



para crear y albergar otro fenómeno reciente, las criptomonedas.

### **Características de blockchain**

Al ser una tecnología novedosa se basa en cadenas de bloques, se destaca por una serie de características.

**La descentralización:** Se refiere a la transferencia del control y la toma de decisiones en una entidad centralizada en una red distribuida, utilizando la transparencia, con el fin de lograr la confianza entre los participantes de esta red.

Para (Jaramillo & Piedra, 2021) La característica de descentralización de esta tecnología, hace posible que las transacciones sean transparentes, de manera que exista trazabilidad en todo el proceso.

**Inmutabilidad:** Una característica especial de esta tecnología es la inmutabilidad, relacionándose directamente con la seguridad de transacciones, esta herramienta se destaca por la imposible alteración de patrones de cada transacción cuando ya se ha registrado en esta red que actúa como un libro de contabilidad.

**Consenso:** En esta tecnología se puede establecer reglas de los bloques con el consentimiento de los participantes de esta red, en donde, solo pueden realizar registros con el consentimiento de todos los participantes.

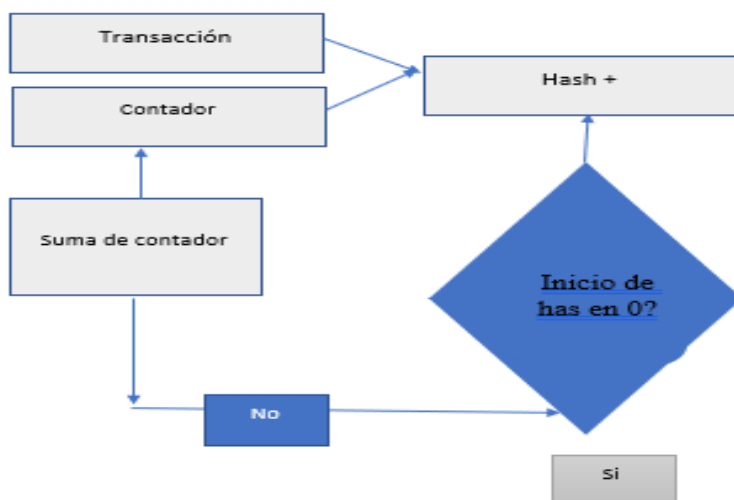


Ilustración 4; Diagrama de consenso Blockchain.

Fuente; Propia

El consenso en blockchain muestra un proceso de minería de Proof of Work, en donde la transacción y el contador, se utilizan para calcular un hash, es decir, si el hash generado empieza con una cantidad específica de transacciones en cero, se incrementa y el contador vuelve a calcular el hash, repitiéndose constantemente para cumplir la condición para que el bloque sea válido y se agrega a la red blockchain.

### **Minería de Proof of Work**

Este término es un tipo de minería de consenso, que se utiliza netamente en la tecnología Blockchain, utilizada para validar y añadir transacciones, básicamente el primero en resolver un problema, es propicio de recibir un nuevo bloque en esta red en una cadena de bloques y recibe recompensas en criptomonedas.

### **Ventajas y desventajas de blockchain**

Para (Villatoro, Velásquez et al, 2021, pág. 22), Esta herramienta, va más allá del uso o aplicación de las criptomonedas como lo es el bitcoin, está, tiene la capacidad de registrar cualquier tipo de transacción financiera embarcándose en el tema de la moneda digital, en donde puede ser bonos, acciones, transferencias de propiedades y cualquier tipo de derecho u obligación.

A pesar que blockchain, es una herramienta beneficiosa para las organizaciones, esta cuenta con ventajas y desventajas en su implementación, variando en un sinnúmero de desventajas que a la vez son beneficiosas para las empresas, pero si no se tiene el suficiente conocimiento de ellas, pasan a ser desventajas con respecto a la seguridad de sus procesos.

- **Ventajas**

1. Blockchain es una herramienta que se caracteriza por tener seguridad reforzada, cada uno de sus datos pueden ser visibles, pero con una incapaz modificación de los mismo, previniendo el fraude y alteraciones de los mismos
2. Cada organización que pone en práctica esta tecnología debe tener una base de datos separada, ya que blockchain se maneja un sistema de registros distribuidos, en donde permite registrar las transacciones de manera idéntica en múltiples ubicaciones, para tener una mayor transparencia.
3. Esta tecnología cuenta con una trazabilidad instantánea, que se refiere a un tipo de auditoría que documenta cada transacción de los activos de esta red, actuando como un libro de contabilidad.
4. Los procesos de blockchain son más eficientes y con mayor velocidad de registro en cada transacción
5. Cada contrato o proceso, se puede automatizar con contratos inteligentes, en donde se proceden a activas una vez cumplido los procedimientos pre establecidos.

- **Desventajas**

1. Dependiendo del volumen de datos y transacciones, esta requiere un mayor almacenamiento.
2. El proceso de transacciones puede ser lento en una cadena de bloques que no esté

centralizada.

3. La integración de blockchain es muy costosa y requiere de tiempo.
4. Los equipos de esta red, consume mayor carga energética.
5. Para la adopción de esta tecnología, requiere personal especializado y de tiempo para un buen manejo de los sistemas.
6. La implementación de claves privadas puede ser un desafío crítico para las personas que no tienen conocimiento en el tema.
7. Los ataques pueden ser filtrados en la red en cadenas de bloques pequeñas y sin seguridad.

### **Blockchain en análisis forense**

Esta herramienta en el análisis forense ayuda a disuadir a delincuentes potenciales que hacen uso de transacciones múltiples para realizar acciones ilegales, gracias a la seguridad de blockchain y su característica centralizada, al detectar actividades ilegales ayuda a mejorar la confianza en finanzas descentralizadas, partiendo desde el análisis de la información de bloques, metadatos y las transacciones realizadas.

Según (Saldaña Taboada, 2023, pág. 122) con mención a investigaciones en materia forense, es necesario hacer un estudio de carácter técnico en tendencias de detección y monitoreo de las transacciones blockchain, partiendo de un punto de vista forense para obtener y descubrir herramientas que faciliten la detección y visualización de resultados.

El análisis forense de blockchain, se basa en un grupo de especialistas sumergidos netamente en temas de redes, encargándose de detectar anomalías en las redes por medio de cualquier dispositivo electrónico para rastrear y dar con el paradero de delincuentes.

Si bien se conoce, para hacer rastreos a nivel de red, ellos tienen que pasar y realizar varios procesos para encontrar anomalías, similitudes y acciones sospechosas en una red Blockchain basada en sistemas financieros de criptomonedas.

## Herramientas de blockchain para el análisis forense

El uso de herramientas para el análisis forense en blockchain es importante debido a los avances tecnológicos en blockchain, en donde ofrecen ventajas y desafíos con respecto al rastreo de delincuentes.

- **Chaunalysis:** Es una herramienta que ofrece una solución en la detección de lavado de dinero o cualquier actividad ilícita, por medio del monitoreo de transacciones y el cumplimiento a cabalidad de normativas establecida.

Según el autor (Kirshner & Schoenberger, 2021), dice que un estudio reciente de blockchain Analytics la empresa Chainalysis, actividad ilícita entre todas las criptomonedas como porcentaje de la actividad total de criptomonedas de 2017 a 2020 fue menos del 1 por ciento específicamente para Bitcoin, la firma de análisis blockchain CipherTrace estima que la actividad ilícita representa menos de 0,5 por ciento del volumen total de transacciones.

- **Elliptic:** proporciona herramientas avanzadas para la detección de actividades ilícitas en blockchain y el cumplimiento de regulaciones AML/KYC, en donde puede llegara identificar transacciones sospechosas, se puede integrar sistemas de cumplimiento de normas y puede llegar a dar detalles d riesgo.

Según (Guodong & Liu, 2022), la matriz de cuantificación se comprime mediante detección de compresión, el tamaño se reduce a la mitad del original y luego las dos matrices comprimidas se unen para formar una nueva matriz. Finalmente, la nueva matriz se cifra mediante cifrado de curva elíptica para obtener la imagen cifrada.

- **Blockseer :** Esta se basa en una herramienta que permite a los investigadores visualizar y por ende analizar las transacciones en una red blockchain, ayudando con la identificación de actividades sospechosas.

Para (Ville, 2023, pág. 8), esto puede convertirse en una amenaza si los reguladores financieros obligan a los mineros a acceder a sus reglas y regulaciones de pendiente resbaladiza,

en donde hay mineros (por ejemplo, Blockseer) que deciden excluir transacciones y direcciones de bitcoin en la lista negra que las autoridades que consideran indeseables.

- **Crystal Blockchain:** basada en una herramienta de blockchain que proporciona un análisis de la red con el fin de detectar anomalías en la red para cuidar la transparencia en cada transacción, siendo utilizada y de mucha ayuda en el análisis forense.

Para (Moreno Martínez, 2022) la Crystal Blockchain o la cadena de bloques de cristal, es una de las herramientas de mayor potencial en materia de seguridad, protección, inviolabilidad e incorruptibilidad de datos, por lo que llegará el inevitable momento de regularla y aprovecharla dentro de la sociedad digital.

### **Algoritmos para el análisis forense de transacciones Blockchain|**

El equipo forense, interconecta diversos algoritmos a la red por medio de una portátil en los servidores, para agilizar los procesos manuales como revisar de forma específica cada transacción hecha, y al ser una red grande de múltiples transacciones está dificultada al ser humano y ralentiza el proceso forense, por ello, optan por hacer uso de tecnologías inteligentes que ayuden en el proceso de detección como lo son también la implementación de algoritmos, pero, los algoritmos que suelen utilizar no son del todo efectivos, ya que las estrategias delictivas son cada vez más innovadoras, encargándose de enmascarar y ocultar transacciones en las redes blockchain para ser ir rastreable, en donde los algoritmos comunes no pueden penetrar en la red para sacar a la luz este tipo de información.

Según (Ramírez Morán, 2021, pág. 25) al ejecutar los algoritmos permiten encontrar el número que da lugar a un bloque validado de transacciones, en donde los forenses recurren a estos algoritmos en una variedad de diferente manera ya que permiten agilizar el rastreo, pero no todos permiten alcanzar tanta eficiencia mediante el uso de dispositivos dedicados.

### **Tipos de algoritmos clustering más utilizados en análisis forense**

- **K-means:** K-means puede agrupar transacciones en clusters basados en características

como montos transferidos y frecuencia de transacciones, siendo rápido y escalable, lo que lo hace adecuado para grandes volúmenes de datos, pero su necesidad de predefinir el número de clusters y su sensibilidad a los outliers pueden ser limitaciones en el rastreo de transacciones.

### Funcionamiento del algoritmo clustering K-means

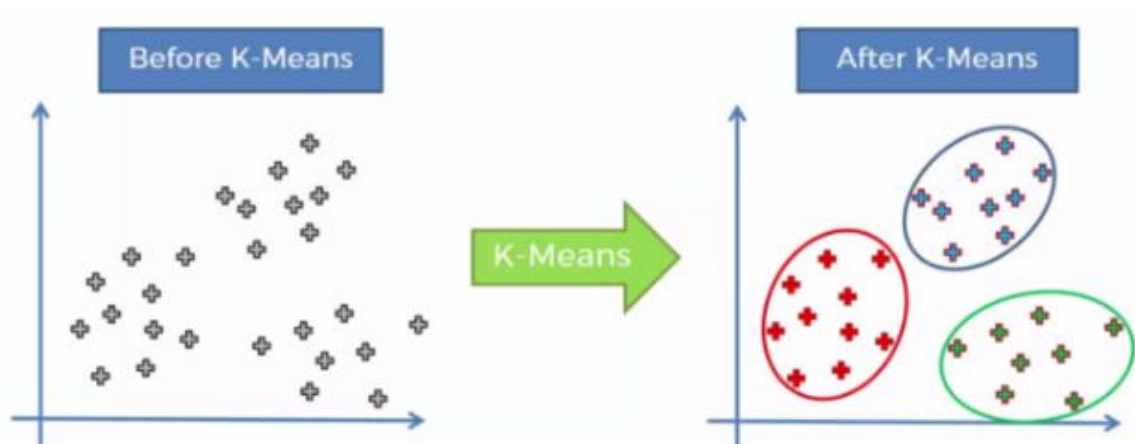


Ilustración 5: Función de k-means

Fuente: (Gliese, 2019)

Esta imagen especifica el funcionamiento de este algoritmo, basándose en la agrupación de datos similares, con el fin de descubrir patrones similares en las transacciones, esto lo hace, buscando un número fijo de agrupamiento clúster en un conjunto de datos en una red, en donde K-means define de inicio el número  $k$  que hace énfasis al número de centroides en los que se dividen los datos en conjunto.

Según (Eghtesadifard, Afkhami, & Bazayr, 2020) se basa en el agrupamiento de transacciones con k-means o k- medidas en donde se clasifica de acuerdo a los requerimientos del personal. Estos algoritmos logran realizar procesos más rápidos en el rastreo de las transacciones en la red blockchain.

- **DBSCAN (Density-Based Spatial Clustering of Applications with Noise):** DBSCAN es particularmente eficaz para detectar clusters de forma arbitraria y manejar ruido (outliers). En el análisis forense de blockchain, DBSCAN puede identificar transacciones densamente conectadas, lo que facilita la detección de

patrones anómalos y actividades sospechosas. No requiere especificar el número de clusters de antemano, lo que lo hace flexible para diferentes estructuras de datos.

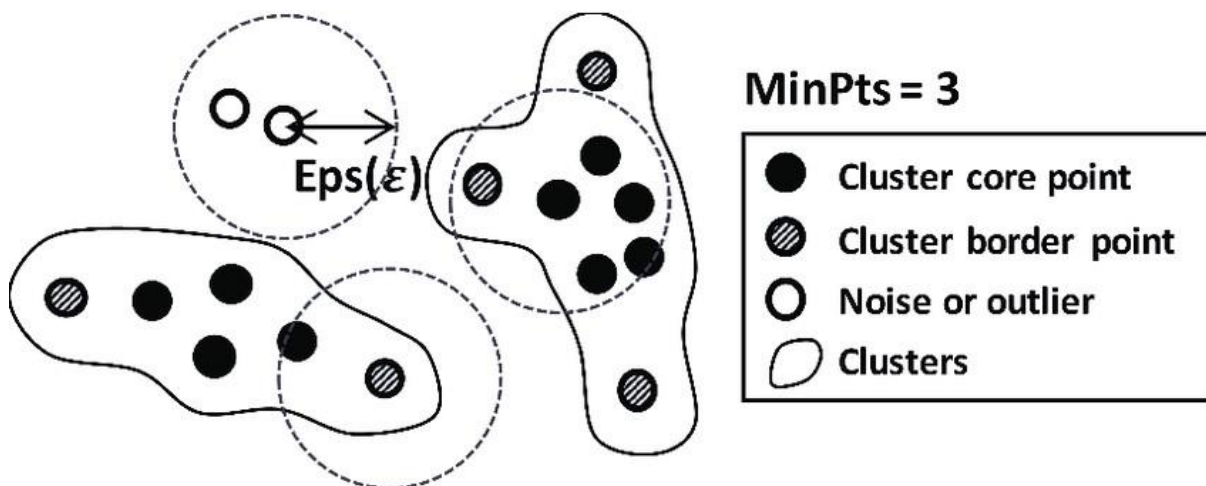


Ilustración 6: Función clúster DBSCAN

Fuente: (Seon , 2019)

Este tipo de algoritmo se basa en la densidad de puntos en un espacio de diversas cantidades de datos, en la imagen se puede visualizar que este algoritmo utiliza dos parámetros claves para cumplir su función EPSe, que es el radio de vecindad y MinPts que es el número mínimo de puntos necesarios a considerar en una región de un clúster.

- **HDBSCAN (Agrupación espacial jerárquica de aplicaciones con ruido basada en densidad):** Este algoritmo jerárquico es útil en blockchain para descubrir estructuras de clusters con densidades variables, comunes en actividades ilícitas complejas, pudiendo identificar clusters de diferentes densidades y tamaños, proporcionando una visión más detallada de los patrones de transacción.

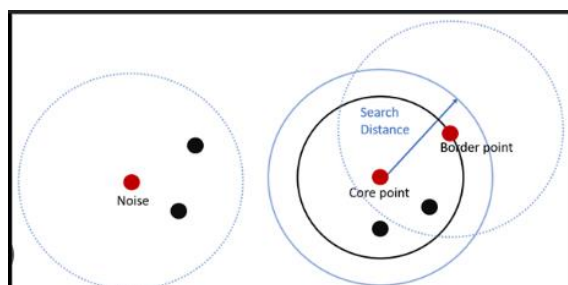


Ilustración 7: Función del clúster basado en densidad o HDBSCAN



Esta imagen representa un clustering de 4 entidades por cada clúster, en donde se tiene cuatro vecinos dentro de la distancia del núcleo de búsqueda, mientras que el vecino tiene tres entidades de búsqueda que son incluidas en un mismo clúster, en mención de las transacciones, asemeja que la búsqueda por medio de este algoritmo en transacciones blockchain, ara que se agrupen las transacciones por distancia y patrón.

Según (Gil Torres, Monroy García, et al, 2020),se basa en la asociacion de diversos objetos de una red,que son especiales en grupos con un alto grado de similitud de transacciones llamadas clusters, las cuales difieren bastante de las características de los objetos pertenecientes a estos, en donde el algoritmo mas importante oara ello es el de agrupacion especial basada en densidad de aplicación.

- **Modelos de mezcla gaussiana (GMM):** GMM asume que los datos son una mezcla de varias distribuciones gaussianas, permitiendo la asignación probabilística de puntos a clusters. En blockchain, GMM puede modelar la distribución de transacciones y detectar anomalías en los patrones, para (Sotaquirá, 2024) este permite realizar tareas de estimación de la distribución de un set de datos de una red o agrupación clustering, ambas teareas son comunes en ciencias de datos y machine learning. Siendo una forma útil para identificar comportamientos sospechosos al considerar la probabilidad de que una transacción pertenezca a un cluster específico.

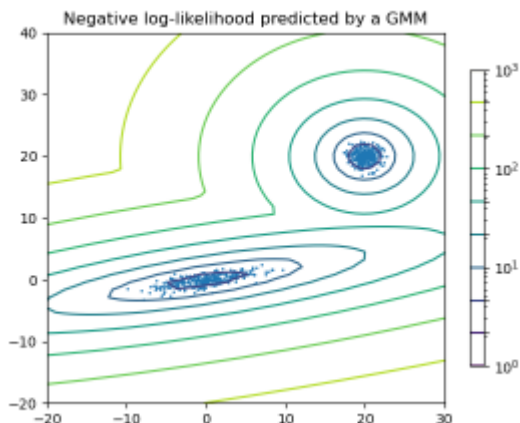


Ilustración 8: Modelo Gussanina

Se basa en un modelo pirobalística de mezcla que asume a todos los puntos de transacciones generados en un número finito de distribuciones gussaninas con parámetros desconocidos en las transacciones.

- **Spectral Clustering:** Según la (Universidad Internacional de La Rioja, 2023) es un proceso muy importante dentro de lo que es machine learning, ya que se basa en la agrupación de datos con características similares y con menor cantidad de errores. Este algoritmo es especialmente útil para estructuras de datos complejas donde las relaciones no son lineales, proporcionando una visión clara de las interconexiones entre transacciones.

Esta imagen representa la técnica en que se realiza el proceso de búsqueda, en donde es netamente basada en la teoría de grafos y la descomposición espectral de las matrices en una lista de transacciones, constituida a partir de grafos de similitudes en datos transaccionales.

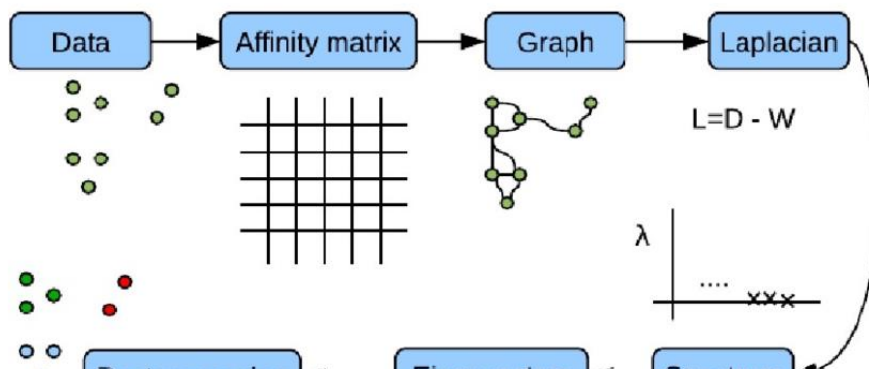


Ilustración 9; Proceso spectral clustering Fuente;

## MARCO METODOLÓGICO

### TIPOS DE INVESTIGACIÓN

**Investigación explorativa:** Esta metodología permite identificar patrones y tendencias ocultas en los datos, revelando relaciones complejas y comportamientos inusuales que no son evidentes a simple vista, facilitando la comprensión de grandes volúmenes de datos, destacando conexiones entre entidades y transacciones, para la eficiencia y precisión en las investigaciones forenses, proporcionando una base sólida para el desarrollo de técnicas más avanzadas.

Para el desarrollo y análisis de este proyecto se utilizó un enfoque integral en donde la virtualización fue de gran ayuda para este estudio, una de las herramientas y software que se utilizaron fue VirtualBox, siendo un software de creación de máquinas virtuales, inicialmente en esta herramienta se instaló Python con cada una de las librerías pandas y scikit-learn pertinentes, en donde estas cumplen la función de recopilación y procesamiento de grandes cantidades de transacciones de una variedad de blockchain.

También se procedió a utilizar Gephi, que es básicamente un software de código abierto, lo que permitió visualizar la estructura de la red y las transacciones que se realizan, este medio, facilitó la detección de la comunidad y los nodos centrales o en este caso máquinas virtuales.

La integración de Power BI, ayudó a interpretar resultados de manera interactiva. Este enfoque no solo permitió identificar patrones sino que también facilita en gran medida la generación de informes de las transacciones.

**Investigación comparativa:** En este punto se procederá a realizar una comparación de los parámetros de los algoritmos K-means, DBSCAN, HDBSCAN, modelo Gaussiana y el spectral clustering, basándose en la capacidad de manejar los datos en altas cantidades dimensionales, la robustez de los algoritmos, la precisión de detectar anomalías con las mismas cantidades de transacciones y por último la escalabilidad, estos resultados serán medidos en un porcentaje de variación de cada uno de los resultados de los algoritmos.

**Método cualitativo:** Permite comprender en profundidad el contexto y las características específicas de las transacciones investigadas, más allá de los números y estadísticas.

**Método bibliográfico:** Este método permite analizar estudios previos, comparando sus hallazgos y metodologías para determinar las mejores prácticas.

### **Técnicas**

**Encuesta:** Permite recopilar y obtener información de las personas que han sufrido estafas relacionadas a sus activos monetarios, en donde se realizará un tablón de preguntas que será impartido por medio de la herramienta de Google formularios

**Muestra:** Esta encuesta fue realizada en la comunidad del Cantón Babahoyo en la Parroquia el Salto, en donde se tomó a una población de a 60 personas, que hacen uso y tienen conocimiento de las criptomonedas, utilizando una variedad de plataformas, en donde realizan pagos y diversas transacciones por este medio.

**Observación:** Con esta técnica ayuda a obtener una observación audaz tanto de las respuestas de la encuesta como la de los algoritmos cloustering.

## RESULTADOS

Como resultado de las encuestas realizada a la comunidad del Cantón Babahoyo en la Parroquia el Salto, se procedió a encuestar a 60 personas, se pudo denotar que una variedad de personas han sufrido de fraudes referentes a las criptomonedas, con un 50% de víctimas en plataformas de Blockchain destacando que un 10% de los mismo no ha experimentado y un 20% no tiene una noción o no están seguros de haber estado sujetos a algún tipo de fraude o estafa,, como bien se expresa, esta pregunta tubo un gran margen de problemática ya que hay un mayor porcentaje de respuestas en donde han sido víctimas de estos acontecimientos y no han tenido soluciones efectivas en diversas ocasiones con respecto al rastreo de sus activos y de dichos delincuentes.

Entre las plataformas mas comunes resaltaron: Bitcoin con un 30%, Ethereum con un 15% y Binance Smart Chain con un 10%, de allí, un 5 % de personas, utilizan otras plataformas, pero la más común es la de Bitcoin, que está tomado fuerza a medida que pasa el tiempo, estando más familiarizada con los pises aledaños.

Estas preguntas base, destacan por ser muy comunes resaltando la prevalencia de fraudes en el ámbito de las transacciones de las criptomonedas, sintiéndose inseguros con el manejo de su moneda virtual en las diversas plataformas, también, en base a la encuesta se manifiesta y denota con un 83% la importancia de mejorar el servicio de rastreo por parte de los profesionales forenses que se especializan en rastrear transacciones de una red blockchain, las plataformas que se dedican a realizar transacciones día a día están en constante actualización por los desarrolladores y es recomendable incorporar a sus análisis de datos, los algoritmos cloustering para tener una mayor eficacia en respuesta y una mejor cabalidad de resultados en el análisis de cada una de las transacciones basándose en la identificación de patrones similares.

En el análisis de los algoritmos clustering, en este estudio se evalúa con los términos de precisión, capacidad de detectar anomalías y la escalabilidad de los mismos en donde tenemos

como resultado.

Para ello se procedió a crear una simulación utilizando VirtualBox en donde se procedió a instalar y configurar paquetes para crear un servidor blockchain, creando una red que consta de tres máquinas, también en el servidor de blockchain se procedió instalar visual estudio code para crear la blockchain con Phyton, node.js , npm y Ganache para simular una blockchain local, y con ello trufflet, entre otros componentes para su óptimo funcionamiento.

Para esto fue necesario un equipo con características prometedoras, en donde se utilizó como sistema operativo Ubuntu 20.04, con un CPU de 5 núcleos, 16 de RAM y un almacenamiento de 100gb, en las máquinas virtuales.

Para la simulación de transacciones en esta red, se hizo necesario crearla con un Scripts usando Web3.js y Web3.py este con el fin de codificar y enviar transacciones.

Al momento de realizar los envíos de transacciones se envió una carga igualitaria y una con dispersión en las 2 máquinas restantes hacia la red, en el primer servidor que está previamente configurada la red, se configuró cada uno de los algoritmos para observar su funcionamiento y agrupación, obteniendo los siguientes resultados comparativos de cada uno de ellos:

<b>Algoritmos Clustering</b>	<b>Precisión %</b>	<b>Detección de anomalías %</b>	<b>Escalabilidad %</b>	<b>Variación en resultados %</b>
<b>K- means</b>	78	65	85	+5
<b>DBSCAN (Agrupación especial basada en densidad)</b>	84	78	70	+3
<b>HDBSCAN (DBSCAN jerárquico)</b>	88	82	75	+4
<b>Gaussian mixture models (GMM)</b>	80	70	80	+6
<b>Spectral Clustering</b>	82	75	72	+5

Tabla 1: Tabla de frecuencia de resultados de algoritmos. Fuente: Propia

Estos resultados fueron obtenidos en base a un análisis de 100 transacciones realizadas, evaluando los porcentajes y resultados de los algoritmos en donde:

- **K- means:** Este algoritmo muestra una mejor escalabilidad, pero su precisión en resultados y detección de anomalías son más bajas en comparación con los demás algoritmos del estudio.
- **DBSCAN (Agrupación especial basada en densidad):** Este algoritmo resalta por tener una alta precisión y una buena detección de anomalías pero tiene una menor escalabilidad debido a la naturaleza del mismo que se basa en una densidad.
- **HDBSCAN (DBSCAN jerárquico):** Destaca en precisión y detección resaltando en ser un algoritmo más efectivo, pero tiene una leve disminución con respecto a la escalabilidad, pero se maneja de mejor manera en resultados.
- **Gaussian mixture models (GMM):** Este algoritmo cuenta con un balance estético con respecto a la precisión y escalabilidad, pero cuenta con una variación en detección.
- **Spectral Clustering:** Resalta en tener un buen desempeño en todas pero su escalabilidad es limitada a diferencia de k-means.

Según este análisis, todos los algoritmos cumplen con su función para lo que es la identificación de transacciones blockchain, en donde HDBSCAN (DBSCAN jerárquico) es más efectivo cuando el enfoque se basa en precisión y detección de las transacciones, por otro lado, k-means sigue siendo el más usado cuando la escalabilidad de las transacciones es una prioridad en el análisis forense, y los demás algoritmos, ofrecen un buen rendimiento pero el algoritmo GMM es más útil cuando el enfoque de la investigación se basa más en probabilidades, este algoritmo es el mejor.

Por otro lado, con respecto a las agrupaciones y manejo de los algoritmos obtuvieron estos resultados.

<b>Algoritmo</b>	<b>Silhouette Score</b>	<b>Ari</b>	<b>Davies Bouldin</b>	<b>Integridad</b>	<b>Homogeneidad</b>
<b>k-means</b>	0.45	0.50	1.75	0.60	0.57
<b>DBSCAN</b>	0.55	0.65	1.30	0.70	0.69
<b>HDBSCAN</b>	0.60	0.70	1.34	0.75	0.74
<b>GMM</b>	0.50	0.55	1.61	0.64	0.62
<b>Spectral Clustering</b>	0.48	0.53	1.68	0.63	0.60

*Ilustración 10: Resultados de agrupación de algoritmos*

*Fuente: Propia*

En mención de **Silhouette Score**, el algoritmo **HDBSCAN**, muestra una mejor agrupación de transacciones con un 0.60 por ciento dentro del clúster, por otro lado, en mención del **ARI**, los algoritmos **DBSCAN** y **HDBSCAN** tiene índices entre 0.65-0.70, siendo más consistentes con respecto a la verdad de terreno analizado al azar de las transacciones.

La **Davies Bouldin**, nuevamente destaca el algoritmo **HDBSCAN** con un 1.35 lo que indica que tiene una mejor separación de los clústeres en las transacciones, también resalta en integridad y homogeneidad destacando y liderando en ambas matrices con un 0.75-0.73, indicando una cohesión interna y buena pureza dentro de las transacciones y los clústeres.



## DISCUSIÓN DE RESULTADOS

**Encuesta:** Según la encuesta realizada, con respecto a los fraudes por medio de la moneda digital, se revelaron problemas emergidos por personas que se dedican a realizar estas actividades ilícitas, en donde, en una mayor cantidad de personas que tienen conocimientos de las criptomonedas o moneda digital, han sufrido estafas, y al optar por la adopción de analistas forense de denoto que los profesionales en este ámbito demoran en dar respuestas pero, esto se debe a las herramientas comunes que muchas veces utilizan para realizar el seguimiento de estas transacciones de una red blockchain, en donde, se hizo evidente según la encuesta, mejorar estas herramientas y por ende proporcionar o implementar el uso de algoritmos clustering en los análisis forenses de esta red, basándose en una mayor obtención de resultados más profundos en cada una de las transacciones eh identificando patrones comunes más efectivos.

**Algoritmos:** En base al análisis de los algoritmos el HDBSCAN, es generalmente el más eficaz para lo que es el rastreo de transacciones forenses, ya que cuenta con una precisión de respuestas de un 88% y una capacidad de detección de anomalías con un 82%, haciéndolo más preciso en la identificación de patrones similares y dar con el paradero eficazmente con el actor, además un factor que le resalta es que maneja eficazmente la variación de densidad y se caracteriza por ser mas robusto en frente te outliers., pero una de sus desventajas en que no es tan rápido en el proceso, pero tiene una escalabilidad del 75% en el análisis de grandes cantidades de datos. El DBSCAN, también puede llegar a cumplir estos parámetros, pero su sensibilidad a ellos y su menor escalabilidad limitan su funcionamiento en cantidades grandes, mientras que K-means se caracteriza por ser más escalable con un 85% pero la precisión y la capacidad de detección son inferiores en comparación con los otros algoritmos, este es más allegado a análisis en una red mas pequeña.

## CONCLUSIONES

Las respuestas de las encuestas, enmarcan una necesidad importante para las personas que hacen uso de la moneda digital, esta red transmite una gran cantidad de transacciones de criptomonedas día a día y las personas que cometen actos ilícitos van en aumento, emergiendo con nuevas estrategias para dificultar el rastreo de las transacciones, y poder ser irrastreable, una de sus estrategias de camuflaje, es realizar múltiples transacciones en diferentes plataformas para hacer más complicado la similitud de cada una de ellas.

En base a los encuestados se resalta la adopción de algoritmos clustering que son más avanzados y con una mayor precisión de respuesta en la similitud de patrones, ya que, en una red blockchain, su función principal, es que cada transacción, es identificada por un patrón que no puede ser modificable una vez hecha en la red.

Por otro lado, los algoritmos clustering son una gran alternativa en las investigaciones forenses, resaltando por arrojar una mayor precisión en anomalías que las herramientas comunes que hacen uso los analistas forenses, ya que en muchas ocasiones la implementación de estos algoritmos en la red puede tornarse difícil, pero es más eficaz en términos de precisión. Existen diversos tipos de algoritmos que cumplen su función, pero el más eficaz es el algoritmo HDBSCAN, siendo más conveniente, por tener un mayor porcentaje en precisión, capacidad de detectar anomalías y la variación de densidad de cargas optando por ser más robusto, pero a pesar que es un poco más lento en respuesta, es más preciso en su búsqueda, para concluir, cada uno de los algoritmos cumple su función y se acoplan a las necesidades de los analistas forenses.

## RECOMENDACIONES

Antes de comenzar la implementación, establece métricas de evaluación como precisión, tasa de falsos positivos/negativos y capacidad de detección temprana, estas métricas te ayudarán a medir la efectividad real de los algoritmos de clustering aplicados a las transacciones blockchain.

Llevar un registro detallado de los comportamientos observados por cada algoritmo, incluyendo los patrones de transacción que detectan mejor las actividades sospechosas, permitirá optimizar la elección de algoritmo según los requerimientos específicos de cada red.

Por otro lado, consultar a especialistas en análisis forense de blockchain y machine learning sirve para identificar qué técnicas de clustering son las más robustas y cómo han sido implementadas en entornos reales.

Por último, revisar cómo cada algoritmo maneja outliers o transacciones atípicas, ya que estos son particularmente importantes para la detección de actividades ilícitas, ya que algoritmos de clustering pueden ignorar estas transacciones o agruparlas incorrectamente, lo cual sería una limitación significativa.

## REFERENCIAS

- Carrera López, J. S., Sánchez Lunavictoria, J. C., & Loza Torres, A. G. (2020). *El uso de la criptomonedas como forma de pago en la economía mundial*. Recuperado el 14 de 06 de 2020, de <https://fipcaec.com/index.php/fipcaec/article/view/228/380>
- Canedo , X. A. (2019). *Importancia de los sistemas informáticos en la toma de decisiones del marketing de las empresas afiliadas a la CAINCO Chuquisaca*. Recuperado el 12 de 6 de 2024, de [http://www.scielo.org.bo/scielo.php?pid=S2521-27372017000200004&script=sci\\_arttext](http://www.scielo.org.bo/scielo.php?pid=S2521-27372017000200004&script=sci_arttext)
- Cargo Suarez, D. (1 de Julio de 2022). Recuperado el 05 de 08 de 2024, de [https://digibuo.uniovi.es/dspace/bitstream/handle/10651/64280/TFG\\_DanielCorgoSua rez.pdf?sequence=4&isAllowed=y](https://digibuo.uniovi.es/dspace/bitstream/handle/10651/64280/TFG_DanielCorgoSua rez.pdf?sequence=4&isAllowed=y)
- Chipolina, S. (2022). *Vendedor de Drogas Con Bitcoin Pagará \$2,3 Millones y 8 Años de Prisión*. Brockton: Decrypt. Recuperado el 1 de 08 de 2024, de <https://decrypt.co/es/95016/vendedor-drogas-bitcoin-8-anos-prision>
- Eghtesadifard, M., Afkhami, P., & Bazayar, A. (2020). *An integrated approach to the selection of municipal solid waste landfills through GIS, K-Means and multi-criteria decision analysis*. Recuperado el 05 de 07 de 2024, de <https://www.sciencedirect.com/science/article/abs/pii/S0013935120302413>
- Fernández, A. (7 de Abril de 2023). Recuperado el 3 de 08 de 2024, de <https://albertofdez.com/blog/seo/que-es-gephi-para-que-sirve/>
- García Arenas, J. (7 de Octubre de 2019). *Blockchain y criptomonedas: bienvenidos al nuevo paradigma*. Recuperado el 1 de 8 de 2024, de <https://www.caixabankresearch.com/es/economia-y-mercados/politica-monetaria/blockchain-y-criptomonedas-bienvenidos-al-nuevo-paradigma-0>

- Gil Torres, A. F., Monroy García, A. L., & González Sanabria, J. S. (19 de Abril de 2020). *Minería de datos espacial en la agricultura en Latinoamérica-Una aproximación conceptual*. Recuperado el 9 de 07 de 2024, de [https://revistas.uptc.edu.co/index.php/pensamiento\\_accion/article/view/10976/9268](https://revistas.uptc.edu.co/index.php/pensamiento_accion/article/view/10976/9268)
- Gliese, T. (15 de Julio de 2019). Recuperado el 2 de 08 de 2024, de <https://exponentis.es/ejemplo-de-clustering-con-k-means-en-python>
- Guodong, Y., & Liu, M. (Septiembre de 2022). *Double image encryption algorithm based on compressive sensing and elliptic curve*. Recuperado el 04 de 07 de 2024, de <https://www.sciencedirect.com/science/article/pii/S1110016821008310>
- Jaramillo, M. P., & Piedra, N. (2021). *Un marco de trabajo basado en tecnología blockchain para mejorar la trazabilidad y la confianza en el intercambio de información entre Instituciones de Educación Superior*. Recuperado el 26 de 06 de 2024, de <https://scielo.pt/pdf/rist/n41/1646-9895-rist-41-97.pdf>
- Jenkinson, G. (2024). *Base de usuarios de criptomonedas supero los 500 millones en 2023*. España: cointelegraph. Recuperado el 30 de 7 de 2024, de <https://es.cointelegraph.com/news/coinbase-full-dismissal-sec-lawsuit>
- Kirshner, J., & Schoenberger, T. (6 de Abril de 2021). *An Analysis of Bitcoin's Use in Illicit Finance*. Recuperado el 04 de 07 de 2024, de <https://cryptoforinnovation.org/wp-content/uploads/2022/07/An-Analysis-of-Bitcoins-Use-in-Illicit-Finance-By-Michael-Morell.pdf>
- Moreno Martínez, A. P. (Sep de 2022). *“Las tecnologías disruptivas frente al principio de seguridad jurídica en materia aduanera”*. Recuperado el 5 de 07 de 2024, de <https://ri-ng.uaq.mx/bitstream/123456789/8627/1/RI007573.pdf>
- Newar, B. (2022). *Los pagos de criptomonedas por ransomware alcanzaron al menos los USD 602 millones el año pasado, revela un informe de Chainalysis*. Chainalysis. Recuperado

el 1 de 8 de 2024, de <https://es.cointelegraph.com/news/ransomware-crypto-payments-hit-at-least-602m-last-year-chainalysis>

Partz, H. (2022). *Bitcoin todavía domina los pagos en BitPay a pesar del mercado bajista*. cointelegraph. Recuperado el 30 de 7 de 2024, de <https://es.cointelegraph.com/news/bitcoin-still-dominates-total-payments-on-bitpay-despite-the-bear-market>

Perez Medina, D. (10 de 2020). *Blockchain, criptomonedas y los fenómenos delictivos: entre el crimen y el desarrollo*. Recuperado el 14 de 06 de 2024, de <https://www.revistas.uma.es/index.php/boletin-criminologico/article/view/11283/11690>

Pérez, S. (8 de Abril de 2024). *Qué es el esquema Ponzi, una variante de estafa piramidal*. Recuperado el 5 de 08 de 2024, de <https://www.newtral.es/esquema-ponzi-estafa-piramidal-que-es/20240408/>

Ramírez Morán, D. (2021). *Dinero digital*. doi:<https://dialnet.unirioja.es/servlet/articulo?codigo=8536452>

Saldaña Taboada, P. (2023). *Análisis criminológico de la delincuencia con criptomonedas cometida por grupos criminales y su aproximación desde los sistemas inteligentes*. Recuperado el 27 de 06 de 2024, de Programa de Doctorado en Criminología: <https://digibug.ugr.es/bitstream/handle/10481/81413/81115.pdf?sequence=4&isAllowed=y>

Seon , H. (2019). *Density-based spatial clustering of applications with noise (DBSCAN)*. Recuperado el 2 de 08 de 2024, de [https://www.researchgate.net/figure/Density-based-spatial-clustering-of-applications-with-noise-DBSCAN-concept\\_fig3\\_331324525](https://www.researchgate.net/figure/Density-based-spatial-clustering-of-applications-with-noise-DBSCAN-concept_fig3_331324525)

Sotaquirá, M. (2 de Enero de 2024). *Modelos de Mezcla Gaussiana: explicación detallada*. Recuperado el 09 de 07 de 2024, de

<https://www.codificandobits.com/curso/probabilidad-nivel-avanzado/8-modelos-mezcla-gaussiana-explicacion-detallada/>

Universidad Internacional de La Rioja. (25 de Abril de 2023). *¿Qué es clustering ?* Recuperado el 09 de 07 de 2024, de <https://ecuador.unir.net/actualidad-unir/clustering-datos/#:~:text=El%20clustering%20es%20un%20proceso,descubrir%20patrones%20o%20detectar%20outliers.>

Villatoro, D., Velásquez, C., Escobar, M., Villatoro, D., & Escobar, A. (Sep-Dic de 2021). *Blockchain en el sector financiero*. Recuperado el 27 de 06 de 2024, de Ventajas y beneficios de la informática y tecnología: <https://incibe.gt/wp-content/uploads/2021/09/Revista-Digital-Cybersecurity-Vol3No2.pdf#page=19>

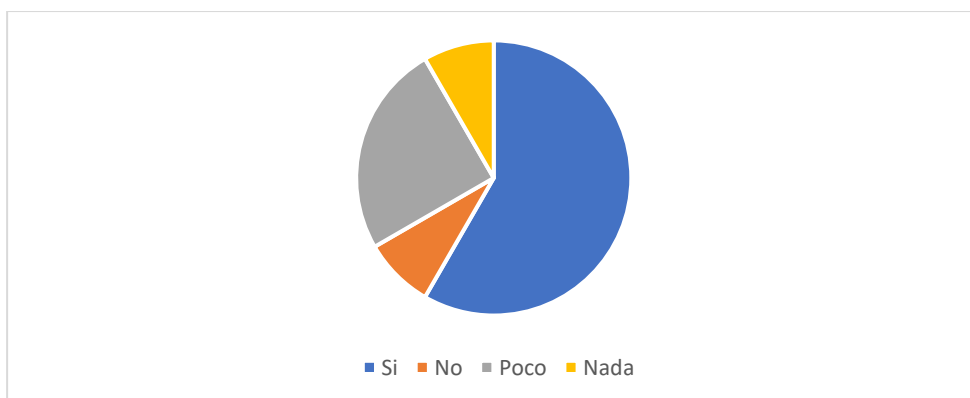
Ville, K. (2023). *Bitcoin as a Nonviolent Tool Against State Financial Censorship*. Recuperado el 04 de 07 de 2024, de [https://www.doria.fi/bitstream/handle/10024/187407/kokkomaki\\_ville.pdf?sequence=2&isAllowed=y](https://www.doria.fi/bitstream/handle/10024/187407/kokkomaki_ville.pdf?sequence=2&isAllowed=y)

## ANEXOS

Esta encuesta fue realizada a 60 personas del cantón Babahoyo, hechas en la parroquia El Salto, en donde su propósito es obtener información sobre las incidencias y percepciones frente al fraude y mal uso de las criptomonedas en una red blockchain, resultando la importancia de contrarrestar este incidente y rastrear las incidencias por parte de los analistas forenses utilizando técnicas e implementando algoritmos clustering como una solución para mejorar el rastreo. Las preguntas tienen un diseño simple y son preguntas cerradas para que sean fáciles de entender, se tomó una muestra de 60 personas, en donde esta muestra se determinó para alcanzar un nivel de confiabilidad del 85% y un margen de error de un 15%, también se realizó un pretest con 10 participantes para reforzar y validar los datos recogidos.

### 1. ¿Tiene conocimiento sobre las criptomonedas o moneda digital?

Opciones	Frecuencia	Porcentaje
Si	35	58%
No	5	8%
Poco	15	25%
Nada	5	8%
Total	60	100%

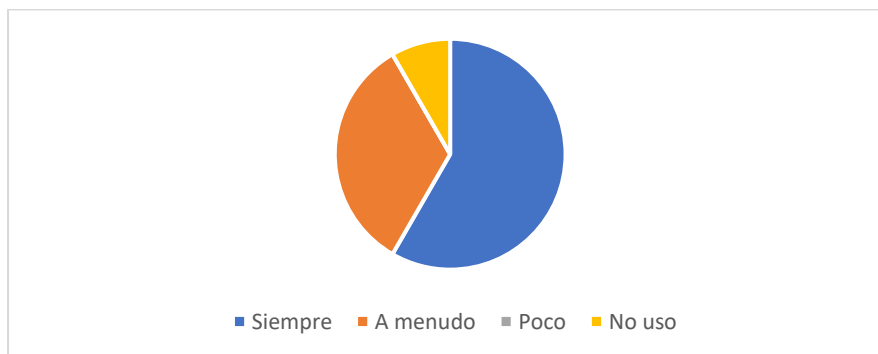


**Análisis;** En la encuesta realizada a 60 personas se pudo observar que el 58% respondió que sí, expresando que si tiene conocimientos o están relacionados con el uso de las criptomonedas en diversas plataformas, mientras que el 15% expresó un conocimiento poco, el 5% no lo tiene y el 5% no tiene nada que ver con esta forma de moneda digital.



**2. ¿Con que frecuencia utiliza las criptomonedas o moneda digital en sus transacciones?**

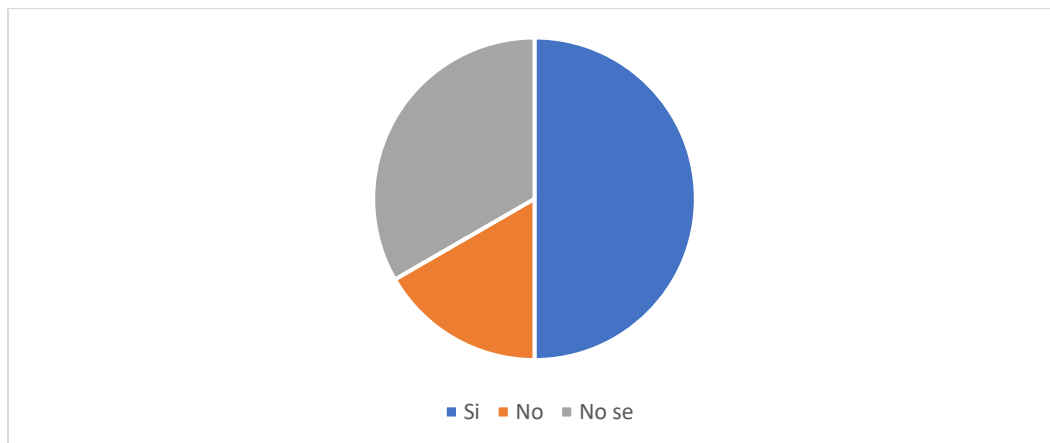
Opciones	Frecuencia	Porcentaje
Siempre	35	58%
A menudo	20	33%
Poco	0	0%
No uso	5	8%
Total	60	100%



**Análisis;** En la encuesta realizada a 60 personas resalta que un 58 por ciento de los encuestados dice que utiliza siempre las criptomonedas en diversas plataformas, mientras que un 33 por ciento dice que la utiliza a menudo y un 8 por ciento no la usa y ninguno de los encuestados opto por la opción de poco, esto quiere decir que hay un uso consecutivo de la criptomoneda para realizar diversas transacciones .

**3. ¿Ha experimentado alguna vez fraudes monetarios digital?**

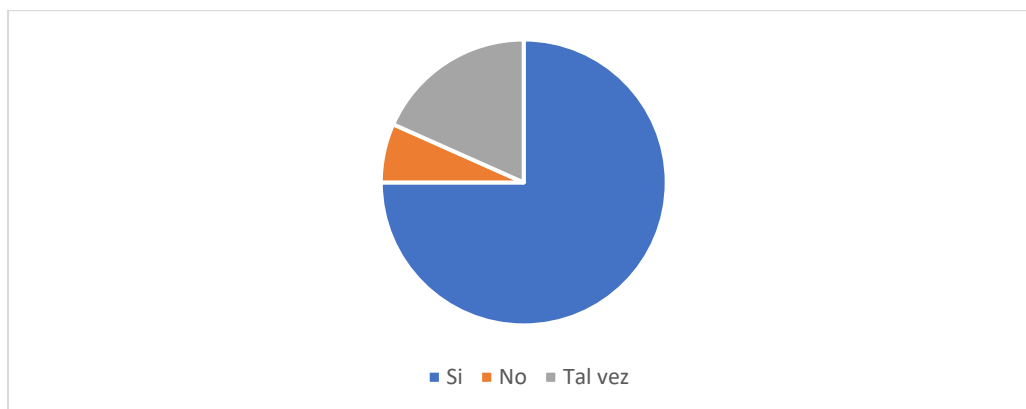
Opciones	Frecuencia	Porcentaje
Si	30	50%
No	10	17%
No se	20	33%
Total	60	100%



**Análisis,** Según este resultado el 50 por ciento de los encuestados ah experimentado fraudes en estas plataformas que hacen uso de las criptomonedas, muestras que un 17 por ciento no lo ha experimentado hasta el momento y un 33 por ciento no tiene noción si lo ha experimentado, esto resalta el aumento de fraudes y mas uso de las criptomonedas en la actualidad, en donde cualquier persona esta propensa a ser víctima.

**4. ¿Usted cree que, en cantidades elevadas de transacciones, es más difícil rastrearlas para llegar con el responsable?**

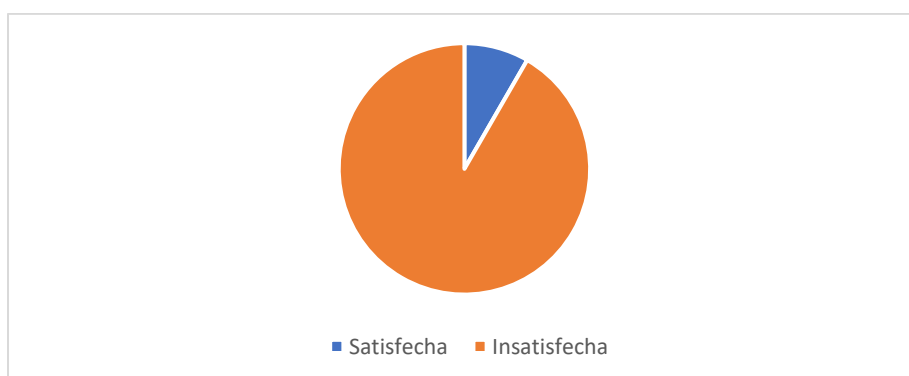
Opciones	Frecuencia	Porcentaje
Si	45	75%
No	4	7%
Tal vez	11	18%
Total	60	100%



**Análisis;** El 45% de las encuestas expresa que, si usa muy a menudo las criptomonedas, mientras que el 4% no lo utiliza y el 11% dijo que tal vez lo usaría, estos resultados expresan que hay un uso frecuente de las criptomonedas en la era moderna y por ende una, mayor inseguridad a la vez para cometer actos ilícitos en esta red.

**5. ¿Qué tan seguro o segura se siente al utilizar criptomonedas en relación con la posibilidad de ser víctima de fraude o alguna actividad ilícita por parte de estafadores?**

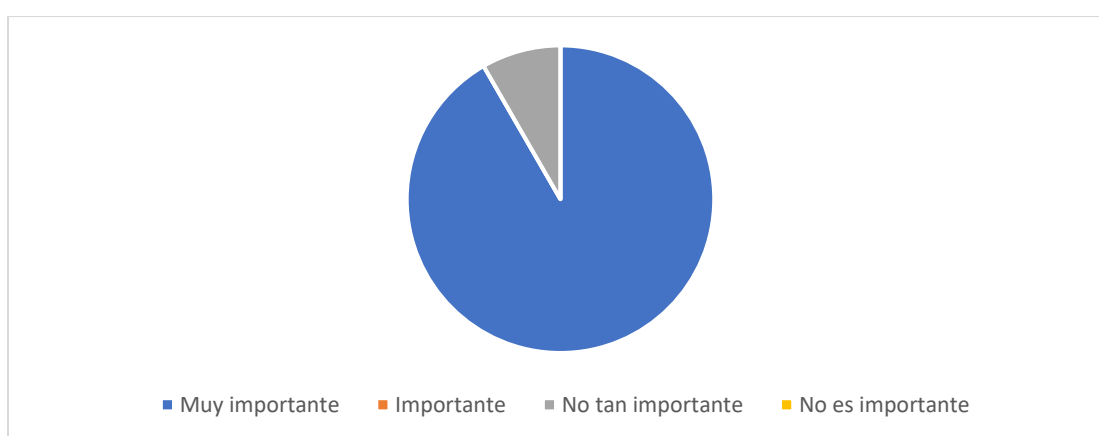
Opciones	Frecuencia	Porcentaje
Satisfecha	5	8%
Insatisfecha	55	92%
Total	60	100%



**Análisis;** el 92% de los encuestados expuso una inseguridad notoria al utilizar las criptomonedas, ya que han experimentado una alta posibilidad de ser víctimas de fraude por su uso y no llegar al paradero de los actores, entre otros, ya que por medio de esta red aparte de estafas, se incentiva el lavado de dinero, mientras que el 8% expresa una satisfacción en su uso.

**6. ¿Qué tan importante considera usted que es mejorar las técnicas de los profesionales en análisis forense para rastrear a las personas que comenten actos ilícitos?**

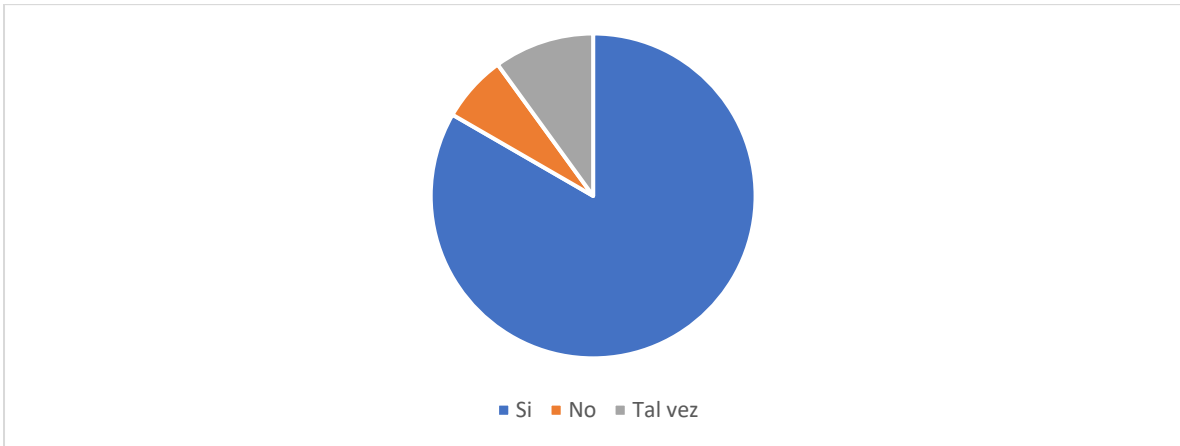
Opciones	Frecuencia	Porcentaje
Muy importante	55	92%
Importante	0	0%
No tan importante	5	8%
No es importante	0	0%
Total	60	100%



**Análisis;** Según los resultados de la encuesta, se revela que para los que usan las criptomonedas y son víctimas de estafas, con un 92% es muy importante mejorar las técnicas que utilizan los analistas forenses para dar con el paradero de las personas que comenten actos ilícitos, esto hace mención al uso de algoritmos clustering como una estrategia de mejora y mejor análisis, el 8% de los encuestados dijo que no es tan importante mejorar estos síntomas.

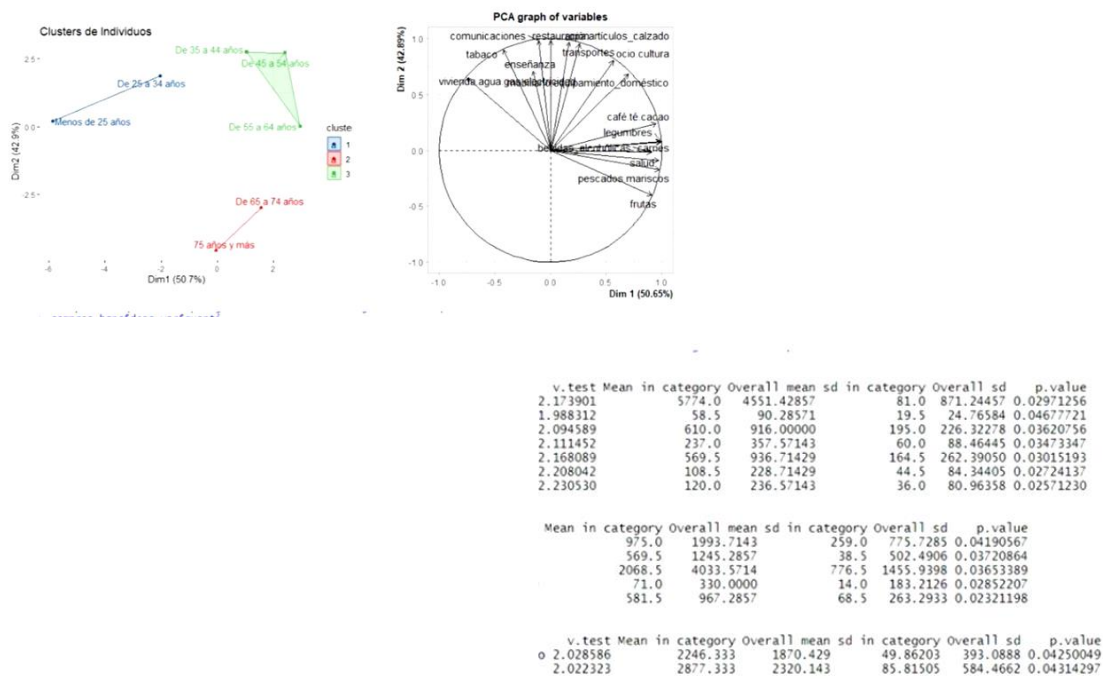
**7. ¿Considera que el uso de algoritmos cloustering en una red blockchain mejoraría el rastreo de transacciones a los forenses?**

Opciones	Frecuencia	Porcentaje
Si	50	83%
No	4	7%
Tal vez	6	10%
Total	60	100%



**Análisis;** El 50 % de los encuestados opto por la opción si, esto significa que el uso de algoritmos clustering mejoraría el proceso de rastreo de actividades ilícitas para el equipo forense, mientras que el 4% no está de acuerdo con la implementación de algoritmos clustering y el 6% sugirió que tal vez ayudaría. Estos resultados expresan una mayor aceptación en el uso y adopción de algoritmos clustering en la red blockchain para el seguimiento de transacciones en esta red.

## ALGORITMO REPRESENTACION DE RESULTADOS DE ALGORITMOS CLUSTERING



Explorer > Bitcoin Explorer > Dirección

1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX USD

**Dirección** USD BTC

Dirección 1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX Contenido patrocinado

Formato BASE58 (P2PKH)

Transacciones 108

Total Recibidas 4.51877366 BTC

Cantidad total enviada 4.26645825 BTC

Saldo final 0.25231541 BTC

Petición de pago Botón de donación

**Transacciones**

Hash 4368b57260f900d465a542fbd03adbeeab... 2017-06-27 14:41  
 354Nv8t86XDF61JZw... 0.84731066 BTC → 1Mz7153HMuxXTuR2R1t... 0.12001000 BTC  
 354Nv8t86XDF61JZw... 0.72631456 BTC

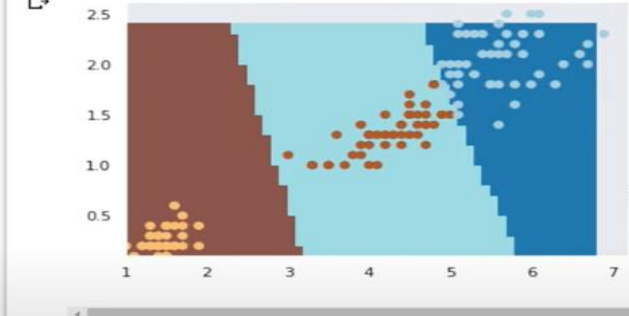
Comisión 0.00098610 BTC +0.12001000 BTC

*Análisis de dirección de bitcoin, transacciones y monto de moneda digital.*

vo Editar Ver Insertar Entorno de ejecución Herramientas Ayuda Se han guardado todos los cambios

+ Código + Texto

"X does not have valid feature names, but"  
 <matplotlib.collections.PathCollection at 0x7feb99161950>



Encontrar numero optimo de clusters

```
[ ] #Encontrando numero de clusters WCSS and elbow method
wcss=[]
```

imple\_data  
po de flores.xlsx

*Agrupamiento transacciones*