



CARTA DE AUTORIZACIÓN

CÓDIGO

AP-BIB-FO-06

VERSIÓN

1

VIGENCIA

2014

PÁGINA

1 de 1

Neiva, 10 de diciembre de 2019

Señores

CENTRO DE INFORMACIÓN Y DOCUMENTACIÓN

UNIVERSIDAD SURCOLOMBIANA

Ciudad

El suscrito:

Juan Felipe Perdomo Guiro, con C.C. No. 1.075.311.940 de Neiva,

Autor(es) de la tesis y/o trabajo de grado o titulado El Fenómeno del *Double Spending* en el Mercado de las Criptomonedas, presentado y aprobado en el año 2019 como requisito para optar al título de Contador Público;

Autorizo al CENTRO DE INFORMACIÓN Y DOCUMENTACIÓN de la Universidad Surcolombiana para que, con fines académicos, muestre al país y el exterior la producción intelectual de la Universidad Surcolombiana, a través de la visibilidad de su contenido de la siguiente manera:

- Los usuarios puedan consultar el contenido de este trabajo de grado en los sitios web que administra la Universidad, en bases de datos, repositorio digital, catálogos y en otros sitios web, redes y sistemas de información nacionales e internacionales “open access” y en las redes de información con las cuales tenga convenio la Institución.
- Permita la consulta, la reproducción y préstamo a los usuarios interesados en el contenido de este trabajo, para todos los usos que tengan finalidad académica, ya sea en formato Cd-Rom o digital desde internet, intranet, etc., y en general para cualquier formato conocido o por conocer, dentro de los términos establecidos en la Ley 23 de 1982, Ley 44 de 1993, Decisión Andina 351 de 1993, Decreto 460 de 1995 y demás normas generales sobre la materia.
- Continúo conservando los correspondientes derechos sin modificación o restricción alguna; puesto que, de acuerdo con la legislación colombiana aplicable, el presente es un acuerdo jurídico que en ningún caso conlleva la enajenación del derecho de autor y sus conexos.

De conformidad con lo establecido en el artículo 30 de la Ley 23 de 1982 y el artículo 11 de la Decisión Andina 351 de 1993, “Los derechos morales sobre el trabajo son propiedad de los autores” , los cuales son irrenunciables, imprescriptibles, inembargables e inalienables.

EL AUTOR/ESTUDIANTE:

Firma: *Felipe Perdomo*

Vigilada Mineducación



**TÍTULO COMPLETO DEL TRABAJO:** El Fenómeno del *Double Spending* en el Mercado de las Criptomonedas

**AUTOR O AUTORES:**

Primero y Segundo Apellido	Primero y Segundo Nombre
Perdomo Guiro	Juan Felipe

**DIRECTOR Y CODIRECTOR TESIS:**

Primero y Segundo Apellido	Primero y Segundo Nombre
Herrera Dussán	Héctor Hernando

**ASESOR (ES):**

Primero y Segundo Apellido	Primero y Segundo Nombre
Herrera Dussán	Héctor Hernando

**PARA OPTAR AL TÍTULO DE:** Contador Público

**FACULTAD:** Economía y Administración

**PROGRAMA O POSGRADO:** Contaduría Pública

**CIUDAD:**

**AÑO DE PRESENTACIÓN:**

**NÚMERO DE PÁGINAS:**

**TIPO DE ILUSTRACIONES** (Marcar con una X):

Diagramas\_\_\_ Fotografías\_\_\_ Grabaciones en discos\_\_\_ Ilustraciones en general X  
Grabados\_\_\_ Láminas\_\_\_ Litografías\_\_\_ Mapas\_\_\_ Música impresa\_\_\_ Planos\_\_\_  
Retratos\_\_\_ Sin ilustraciones\_\_\_ Tablas o Cuadros X



**SOFTWARE** requerido y/o especializado para la lectura del documento:

**MATERIAL ANEXO:**

**PREMIO O DISTINCIÓN** (*En caso de ser LAUREADAS o Meritoria*):

**PALABRAS CLAVES EN ESPAÑOL E INGLÉS:**

<u>Español</u>	<u>Inglés</u>	<u>Español</u>	<u>Inglés</u>
1. Doble gasto	Double spending	6. Fraude financiero	Financial fraud
2. Criptomonedas	Cryptocurrencies	7. Mineros	Miners
3. Bitcoin	Bitcoin	8. Regulación	Regulation
4. Blockchain	Blockchain	9. Problema	Problem
5. Economía	Economy	10. Sistema	System

**RESUMEN DEL CONTENIDO:** (Máximo 250 palabras)

El doble gasto es un problema económico presente solo en las monedas virtuales, es utilizado por personas mal intencionadas para desestabilizar el sistema de las criptomonedas y a través de este fraude sacar ventajas de tipo personal. *Bitcoin* fue la primera criptomoneda en combatir este problema por medio de la tecnología *Blockchain* en donde se lleva un registro de todas las transacciones de la plataforma evitando con esto que dos transacciones sean aceptadas cuando en realidad solo se puede cubrir una de las dos.

Es posible que el doble gasto pueda traer consecuencias contundentes al sistema contable de cualquier compañía que sufra un ataque de estos, a tal punto de propiciar su liquidación dependiendo de la magnitud de este fraude.



**ABSTRACT:** (Máximo 250 palabras)

The double spending is an economic problem present only in virtual currencies, it is used by cyber criminals to destabilize the cryptocurrency system and through this fraud take personal advantages. Bitcoin was the first cryptocurrency to combat this problem through blockchain technology where a record of all platform transactions is kept, thereby preventing two transactions from being accepted when only one of the two can be covered.

It is possible that the double expense can bring strong consequences to the accounting system of any company that suffers an attack of these, to the point of promoting its liquidation depending on the magnitude of this fraud.

**APROBACION DE LA TESIS**

Nombre Presidente Jurado: Ricardo León Castro Zamora

Firma:



RICARDO LEÓN CASTRO ZAMORA  
Presidente

Nombre Jurado: Ramiro Peralta Morales

Firma:



RAMIRO PERALTA MORALES  
Docente -Jurado



DESCRIPCIÓN DE LA TESIS Y/O TRABAJOS DE GRADO

CÓDIGO

AP-BIB-FO-07

VERSIÓN

1

VIGENCIA

2014

PÁGINA

4 de 4

Nombre Jurado: Cristian Felipe Orjuela Yacue

Firma:



CRISTIAN FELIPE ORJUELA YACUE  
Docente-Jurado



EL FENÓMENO DEL *DOUBLE SPENDING* EN EL MERCADO DE LAS  
CRIPTOMONEDAS

JUAN FELIPE PERDOMO GUIRO  
ESTUDIANTE

HÉCTOR HERNANDO HERRERA DUSSÁN  
DIRECTOR

PROYECTO PARA OPTAR POR EL TÍTULO DE CONTADOR PÚBLICO

UNIVERSIDAD SURCOLOMBIANA  
FACULTAD DE ECONOMÍA Y ADMINISTRACIÓN  
CONTADURÍA PÚBLICA  
NEIVA - HUILA  
2019

**Nota de aceptación**

---

---

---

---

---

RICARDO LEÓN CASTRO ZAMORA  
Presidente

---

CRISTIAN FELIPE ORJUELA YACUE  
Jurado

---

RAMIRO PERALTA MORALES  
Jurado

Neiva, Huila

## ÍNDICE

1. ANTECEDENTES.....	5
1.1 Planteamiento del problema.....	12
2. OBJETIVOS.....	16
2.1 Objetivo General.....	16
2.2 Objetivos Específicos.....	16
3. JUSTIFICACIÓN.....	16
4. MARCO REFERENCIAL.....	20
5. DISEÑO.....	57
5.1 Clase de investigación.....	57
5.2 Metodología de la investigación.....	57
5.2.1 <i>Situación de la problemática</i> .....	58
5.2.2 <i>Modelo de análisis utilizado</i> .....	58
5.2.3 <i>Resultados</i> .....	58
5.3 Muestreo.....	58
5.3.1 <i>Clases de muestreo</i> .....	58
5.3.2 Población.....	59
5.3.3 Muestra.....	59
5.4 Instrumentos para la recolección de datos.....	59
5.4.1 <i>Herramientas para situación problema</i> .....	59
5.4.2 <i>Herramientas modelo análisis</i> .....	59
5.4.3 <i>Resultados</i> .....	60
5.5 Recursos.....	60
5.5.1 <i>Materiales de investigación</i> .....	60
5.5.2 <i>Recursos humanos</i> .....	61
6. FINANCIACIÓN.....	61
7. CRONOGRAMA.....	62
8. DATOS.....	63
9. ANÁLISIS DE LOS DATOS.....	68
10. RESULTADOS Y CONCLUSIONES.....	75
BIBLIOGRAFÍA	
ANEXOS	

## LISTA DE TABLAS

Tabla N. 1. Registro contable de una inversión por persona natural.....	53
Tabla N. 2. Registro contable del dinero perdido por un ataque de doble gasto.....	53
Tabla N. 3. Registro contable del retiro de la inversión.....	54
Tabla N. 4. Materiales de investigación.....	60
Tabla N. 5. Recursos humanos.....	61
Tabla N. 6. Financiación.....	61
Tabla N. 7. Cronograma.....	62
Tabla N. 8. Documento N. 1.....	63
Tabla N. 9. Documento N. 2.....	64
Tabla N. 10. Documento N. 3.....	65
Tabla N. 11. Documento N. 4.....	66
Tabla N. 12. Documento N. 5.....	67
Tabla N. 13. Entrevista doble gasto.....	68
Tabla N. 14. Documentos seleccionados para el análisis documental.....	69
Tabla N. 15. Formas de control sobre el <i>double spending</i> .....	70
Tabla N. 16. Caracterización del <i>double spending</i> .....	71
Tabla N. 17. Funcionamiento del <i>double spending</i> .....	72
Tabla N. 18. Regulación legal y normativa... ..	73
Tabla N. 19. Panorama local del <i>double spending</i> .....	74
Tabla N. 20. Ataques de doble gasto en Colombia.....	75

## EL FENÓMENO DEL *DOUBLE SPENDING* EN EL MERCADO DE LAS CRIPTOMONEDAS.

### 1. ANTECEDENTES

El desarrollo de la tecnología en el siglo XXI ha propagado un cambio de paradigma en muchos aspectos de la vida, incluida la economía global, desarrollando nuevas formas de intercambiar bienes y servicios. Este cambio avanzó hasta llegar a la implantación de las nuevas tecnologías sumergidas en el mundo de la economía. Una de estas nuevas formas para realizar las operaciones económicas es a través de las criptomonedas, las cuales cumplen un papel similar al del dinero pero en el mercado electrónico; sumado a ello es imperativo agregar que el *Bitcoin* es la criptomoneda más reconocida a nivel mundial, pues fue la primera moneda digital utilizada para realizar este tipo de transacciones y desde su creación en el 2009 el uso de la misma ha ido en aumento, por lo cual algunas naciones han tomado cartas en el asunto, para regular su funcionamiento.

Estados Unidos fue una de las primeras naciones en respaldar las operaciones en *Bitcoins* al no considerarlas ilegales, la agencia federal las consideró como un medio legal de cambio, además, surgieron leyes que rigen productos, servicios y transacciones relacionadas con esta moneda digital. Por otra parte, es importante agregar que el primer cajero automático para *Bitcoin* fue instalado en Vancouver (Canadá), ofreciendo dólares canadienses a cambio de criptomonedas; se evidencia que en el norte del continente americano le han dado un apoyo a este nuevo mercado digital. (Pallares, 2014).

Para el Banco Central Europeo el *Bitcoin* es un tipo de dinero no regulado por ninguna autoridad centralizada, que es emitido y regulado en forma digital por sus propios creadores, usadas y aceptadas según la confianza que genera entre los miembros de una comunidad virtual específica. (Rivas, 2016). De la misma manera, la Comisión Europea

apoyó este sistema implementando un observatorio para explorar las oportunidades que tendría la aplicación del mismo, la Unión Europea eximió al *Bitcoin* de los impuestos al valor agregado y algunos países están contemplando mejoras en sus marcos regulatorios para las criptomonedas.

*“(...) En el caso de Alemania, el gobierno declaró en junio del 2013 que el Bitcoin sería tratado como una actividad comercial y que estaría sujeto a impuestos relacionados con las rentas obtenidas, a menos que estas fueran mantenidas por un periodo superior a un año. Del mismo modo, la regulación en Reino Unido y España exigen el pago del IVA a las transacciones de Bitcoin, mientras que Noruega no lo ha reconocido como moneda, aunque sí impone una tasa sobre los beneficios obtenidos o una desgravación en caso de pérdidas”.* (CEF, 2017).

Por otra parte, Islandia restringe el comercio exterior de *Bitcoins* pero los ciudadanos Islandeses pueden poseerlas y usarlas dentro de ese país; en Rusia también están prohibidas y su uso se considera ilegal. (Arango, 2018).

Una mirada hacia los países orientales demuestra que en Japón se han creado políticas en cuanto a este tema para controlar el auge que han tenido las mismas, se reconocen como medio de pago e incluso cuenta con compañías operadoras de criptomonedas oficiales. En China, las operaciones en casas de cambio han sido bloqueadas al igual que la publicidad en internet de las mismas; sin embargo, los usuarios pueden comprarlas y venderlas por la red, sin que intercedan los bancos. El gobierno de la India prohibió la comercialización de criptomonedas y su relación con entidades bancarias.

Las autoridades financieras de Corea del Sur presentaron el plan fiscal para cobrar impuestos a las criptomonedas a partir de este año, a pesar de que un inicio se buscaba

bloquear todo tipo de actividad relacionada con este tema. Por otro lado, el Banco Central de Bangladesh no permite el uso de plataformas para realizar actividades con *Bitcoins* y advierte de los riesgos a quienes las utilicen por fuera.

Los países latinoamericanos tampoco tienen claridad acerca de las criptomonedas y se encuentran diversas opiniones; México por ejemplo ha creado instituciones que deben hacer advertencias a los usuarios sobre los riesgos relacionados con la operación a través de criptomonedas; el Banco Central de Brasil ha advertido que las monedas digitales aún no cuentan con la estabilidad necesaria para considerarse un valor o un medio de intercambio seguro y legítimo; en Argentina se afirma que no son emitidos por bancos centrales ni por otras autoridades monetarias internacionales y, por lo tanto, no tienen curso legal. Bolivia prohibió totalmente el uso y tenencia de las mismas y el Banco Central de Ecuador no las autoriza como medio de pago de bienes y servicios.

*“(...) El Banco Central de Chile expresa que las monedas virtuales no cuentan con un reconocimiento legal o reglamentario específico y que la actividad de compraventa o intermediación de estas no está sujeta a la potestad regulatoria de este organismo y este mercado está fuera del perímetro regulatorio de la Unidad de Análisis Financiero”. (CEF, 2017).*

En Uruguay al igual que en muchos países del mundo la situación es incierta, pues el gobierno aún no se ha pronunciado al respecto para declarar las criptomonedas legales o ilegales en su economía, y solo pueden ser utilizadas por personas naturales con proyección de inversión y especular sobre esta clase de moneda.

Es importante tocar el tema de Venezuela, ya que es bastante particular, debido a que el mismo Gobierno estipuló a inicios de 2018, una moneda virtual denominada “petro-

activo”, cuyo fin fue facilitar el ejercicio de compra y venta de su petróleo, lo cual se complejizó a causa de la significativa desvalorización que sufrió su moneda oficial: los bolívares. Durante el 2019, solo en el país en mención ya se han intercambiado 16.662 *Bitcoins* a través de Localbitcoins. (Cámara de Comercio de Bogotá, 2018).

En la actualidad, las criptomonedas han acogido una fama significativa y algunas empresas muy importantes a nivel mundial las han empezado a utilizar en sus plataformas y a aceptarlas como medio de pago, siendo algunas de ellas: *Subway, KFC, Paypal, Expedia, Dish Network, Dell y Microsoft*.

En el mundo, hay registrados 14.442 comercios relacionados con *Bitcoin*. En Neiva se estima que existen 5 establecimientos en los cuales se pueden comercializar con ellas, Bogotá (120) y Medellín (36) son las ciudades colombianas con más sitios en los cuales se pueden utilizar criptomonedas. En Europa y Norteamérica se evidencia la mayor cantidad de negocios de ese tipo, pueden encontrarse restaurantes, almacenes de ropa, tiendas deportivas y otros tipos de sectores. (Coinmap, 2019).

El marco regulatorio alrededor de las criptomonedas y especialmente del *Bitcoin* está muy dividido en todo el mundo, desde países que le han dado un espaldarazo a este sistema mediante la creación de leyes que las regulan e incluso cajeros automáticos de *Bitcoins* y otros en donde lo han prohibido en el sistema bancario sin la posibilidad de usarla en el intercambio de bienes y servicios; sin embargo, en la mayoría de países son insuficientes las medidas para controlar esta moneda digital debido a la falta de información sobre cómo regular este fenómeno y la poca experiencia en este sistema digital.

Lo anterior refleja un panorama del marco regulatorio a nivel mundial de las criptomonedas, pero es necesario dar una definición de este tema para tener un panorama

claro de lo que se está hablando, por esa razón se definen de la siguiente manera: las criptomonedas (también conocidas como monedas virtuales) son un nuevo tipo de dinero digital descentralizado que puede utilizarse para realizar pagos, compras o diversas inversiones en el mercado global, estas monedas son guardadas, negociadas y transferidas electrónicamente.

Dentro de este amplio tema, se encuentran una variedad inmensa de las mismas, más de 2000 en la actualidad, entre las que se hallan el *Ethereum*, *XRP*, *Litecoin*, *Tron*, *Teller*, *Dash*, *Monero*, entre otras; siendo la más sobresaliente el *Bitcoin*, “*la cual es una moneda virtual que funciona como un sistema de pagos basado en archivos de computador, y como tal sirve para transar de manera encriptada bienes y servicios o para realizar transferencias de valor. Por su condición de archivo puede ser destruido o perdido, igual que el dinero*”. (Rivas, 2016). A lo largo de la historia se han evidenciado serios problemas en el sistema de las criptomonedas que ponen en riesgo su funcionamiento y credibilidad, desde la competencia con el sistema bancario tradicional, su relación con actividades ilícitas como evasión, fraude y lavado de dinero, pero el problema central es el doble gasto (*double spending*), que consiste en que un usuario malicioso de la red puede crear dos transacciones correctas separadas la una de la otra, de manera que realice simultáneamente dos compras para las cuales tiene fondos para cubrir individualmente, pero no para las dos juntas. A este problema se le ha denominado como “problema del doble gasto”.

Cuando un archivo es enviado a través de internet, la propagación de este sobre la red habilita la creación de infinitas copias del mismo, por lo que, si se considera usar un archivo digital como moneda, podría copiarse y realizar diversos pagos con un mismo archivo, lo que lo volvería inútil para funcionar como dinero, esto se conoce como: “el doble gasto”.

Después de abordar el tema a nivel global y tener una idea de las definiciones más importantes es necesario indagar en el ámbito colombiano, donde dos de las instituciones fundamentales en términos financieros, el Banco de la República y la Superintendencia Financiera, ya se han pronunciado al respecto, pero sus posturas no han sido suficientes ni contundentes, dejando muchas preguntas sin resolver.

En la situación colombiana, la Superintendencia Financiera y el Banco de la República han desarrollado comisiones especiales para realizar un análisis exhaustivo del tema; sin embargo, a la fecha todavía no se han hecho públicas las normativas oficiales al respecto, generando un escenario de incertidumbre y duda respecto al tema en cuestión. Las operaciones con criptoactivos en el país no están prohibidas, pero estas no cuentan con el respaldo del estado y las autoridades económicas advierten con frecuencia sobre los riesgos y peligros que se pueden hallar al hacer uso de este sistema financiero. (CR Consultores Colombia, 2017).

El Banco de la República, por medio de un comunicado de prensa, afirma que el *Bitcoin* no es una moneda en Colombia y por esa razón no hay obligatoriedad de recibirlo como medio de pago de las obligaciones; allí mismo, reafirma como única unidad monetaria el peso emitido por esta misma entidad. El “Comunicado *Bitcoin*” emitido el martes 1 de abril de 2014 contiene lo siguiente:

El Banco de la República se permite informar que:

1. La única unidad monetaria y de cuenta en Colombia es el peso (billetes y monedas) emitido por el Banco de la República.

2. El *Bitcoin* no es una moneda en Colombia y, por lo tanto, no constituye un medio de pago de curso legal con poder liberatorio ilimitado. No existe entonces obligatoriedad de recibirlo como medio de cumplimiento de las obligaciones.

3. El *Bitcoin* tampoco es un activo que pueda ser considerado una divisa debido a que no cuenta con el respaldo de los bancos centrales de otros países. En consecuencia, no puede utilizarse para el pago de las operaciones de qué trata el Régimen Cambiario expedido por la Junta Directiva del Banco de la República. (Banco de la República, 2014).

Por su parte, la Superintendencia Financiera de Colombia prohibió a las entidades que estén bajo su supervisión realizar operaciones con *Bitcoins* y restringe cualquier relación con monedas virtuales debido a que no se encuentran reguladas por la ley colombiana, es decir, que las personas que quieran incursionar en este mercado lo harán bajo su responsabilidad y no deben estar bajo el control de la Superintendencia Financiera. La Carta Circular 029 de 2014 fue contundente al comunicar lo siguiente:

*“(...) Finalmente, esta Superintendencia recuerda que las entidades vigiladas no se encuentran autorizadas para custodiar, invertir, ni intermediar con estos instrumentos. Adicionalmente, corresponde a las personas conocer y asumir los riesgos inherentes a las operaciones que realicen con las “monedas virtuales”.* (Superintendencia Financiera de Colombia, 2014).

En ningún momento se declara ilegal el *Bitcoin* para las personas que no son vigiladas por la Superintendencia Financiera de Colombia; sin embargo, los particulares que utilicen esta moneda virtual deben conocer los riesgos y peligros a los que se exponen. Otro

punto a destacar es que ninguna de estas entidades dio un apoyo fundamental a este sistema, motivo por el cual deja muchos interrogantes relacionados con su utilización.

Se puede llegar a pensar que estas dos entidades financieras se están interponiendo en el avance de las criptomonedas en el territorio nacional ya que no están contribuyendo a su regulación para su posterior avance; sin embargo, se debe tener en cuenta los riesgos que pueden traer a la economía del país y que de alguna manera la Superintendencia Financiera de Colombia y el Banco de la República deben primero pensar en mitigar estos peligros.

Por otra parte, algunos senadores de la república están considerando regular el uso de las monedas virtuales y las formas de transacción en el país por medio de un proyecto de ley para presentar ante el Congreso, pese a ello, esta acción ha recibido muchas críticas ya que algunos expertos afirman que algunas propuestas van en contravía del uso de las mismas, se limitan los actores y el impuesto con el que se gravarán no es del agrado de muchos. Se evidencia una preocupación en algunos sectores por las inconsistencias y deficiencias del documento, todo esto ante la falta de conocimiento acerca del tema.

### **1.1 Planteamiento del problema**

En toda la historia se han presentado ciertos tipos de peligros en los diferentes sistemas económicos como la desestabilización del sistema bancario y de las instituciones, las tensiones geopolíticas, los altos niveles de endeudamiento, el aumento de la incertidumbre, entre otros, que ponen en jaque su funcionamiento.

Las primeras monedas virtuales emitidas no contaban con un mercado estable, ni la aceptación de las personas dada la especulación y la poca credibilidad y confiabilidad del sistema, pese a ello, hoy en día parece un tema muy atractivo y en el cual los gobiernos y los

bancos ya se han preocupado por este tema debido a su auge en la sociedad y se han visto obligados a tomar medidas para regular este fenómeno.

Las criptomonedas se han identificado como la solución al comercio digital pero no han sido ajenas a los riesgos, enfrentando fraudes que han intentado desestabilizar por completo este sistema, dejándole pérdidas millonarias y perdiendo la credibilidad de los partícipes.

Debido a que ningún intermediario verifica la legalidad de las transacciones y la identidad anónima de quienes participan en el mercado, las criptomonedas se han convertido en el blanco perfecto para emplearse con fines de lavado de dinero y financiamiento del terrorismo.

El riesgo de quienes participan en el sistema de las criptomonedas es significativo, debido a que no se tiene respaldo de ninguna autoridad monetaria y legal en el mundo, la aceptación para efectuar pagos restringe el uso de las mismas como medio de intercambio, además la incertidumbre que se maneja en este mercado es absoluta por su valor tan volátil, por eso se deben tener muy claro las posibles maneras en que las personas inescrupulosas pueden blanquear las monedas virtuales.

Este sistema debe afrontar serios desafíos para regular un mejor funcionamiento y una mayor seguridad en las transacciones, entre lo que se encuentran: el control de lavado de activos y financiación del terrorismo, protección del consumidor y los recursos públicos, alta volatilidad de precios y aspectos financieros, manejo cambiario y los flujos de capitales, aspectos fiscales y tributarios del país y la soberanía monetaria y estabilidad financiera. (Arango, 2018).

Uno de los mayores peligros a los que se han tenido que enfrentar los usuarios de las criptomonedas es el problema del doble gasto, cuyo fin radica en adquirir dos bienes o servicios con la utilización de la misma transacción, es decir, que no tiene suficiente valor adquisitivo para obtener los dos bienes o servicios por separado, sin duda alguna esta forma de estafa provoca millones de pérdidas a los actores de este mercado y la caída en el precio de las criptomonedas se ve afectado. En palabras más convencionales es la forma en que una persona gasta dos veces el mismo dinero generando un escenario de estafa.

Para mitigar este grave fenómeno, se hizo necesario crear un sistema contable público descentralizado llamado “*Blockchain*”, el empezó a ejercer un control de todas las transacciones que se realizaban y de esta manera evitar que la misma unidad de valor se utilice para suplir dos gastos, el sistema *Blockchain* está ligado al *Bitcoin*, que como ya se dijo anteriormente es la criptomoneda más reconocida en el mundo.

*“(...) Para asegurar que no se gaste dos veces la misma criptomoneda, cada miembro de la red verifica y valida las transacciones empleando tecnologías derivadas de la informática y la criptografía. Cuando se logra la unanimidad entre los miembros de la red, la transacción se añade al registro, validando la misma”.*

(Fondo Monetario Internacional, 2018).

Dentro de los datos históricos sobre este tema en particular se encontró que el 18 de mayo del 2019, un minero malintencionado ejecutó con éxito un ataque a este sistema en la red *Bitcoin Gold*, haciendo que esta criptomoneda estuviera sometida a un ataque de red durante ese día. Inicialmente, el *Blockchain* resolvería este problema, pero el minero obtuvo por un tiempo el control del mismo al adquirir el 51% de la potencia total de la red, lo cual le permitió revertir las transacciones y robar fondos de los intercambios de criptomonedas,

este es solo uno de los diversos ataques que han sufrido de esta manera diversas clases de criptomonedas. (Pérez, 2018).

En otro caso de ataque, los servicios *on line* ofrecidos por la Universidad St. Francis Xavier (Canadá) permanecieron aislados durante la mayor parte de los primeros días del mes de noviembre de 2018 debido a un ciberataque para extraer *Bitcoin* y obtener ganancias monetarias, confirmado en los recursos informáticos de la universidad. El ataque llevó al cierre temporal del sistema de cursos *on line* de la universidad, almacenamiento en la nube, servicios de correo electrónico, transacciones de débito y *wifi*. Así mismo, la casa de cambio neozelandesa Cryptopia ha sido víctima de varios ataques, en el último le fueron robados 1.675 Ethereum, lo que equivale alrededor de 180.000 dólares. Esto demuestra lo poco confiable de esta plataforma ya que no se tiene control sobre las llaves privadas de los monederos. (Esparragoza, 2018).

El *Blockchain* permitió tener un mayor grado de seguridad en las transacciones; sin embargo, se evidencian falencias como en los casos mencionados anteriormente y por eso es necesario indagar acerca del problema del doble gasto para conocer de cerca todo este sistema y su reflejo en la economía por sus masivos fraudes y estafas a los que han estado expuestos los usuarios.

Sin duda alguna esta tecnología representa una revolución a nivel global por el posible impacto que puede generar en sectores económicos de la sociedad, así como en la educación, auditorías, mercados financieros, entre otros.

La tecnología *Blockchain* trae consigo unas ventajas, la más importante de ellas es la transparencia y seguridad en los procesos, además permite que los procesos sean mucho más eficientes y con una reducción importante en los costos.

El problema del doble gasto es provocado por cibercriminales que quieren aprovechar las debilidades del sistema para sacar ventajas personales como el aumento de su capital a través del blanqueo de otras cuentas, desencadenando en una baja significativa del precio de la moneda virtual y por consiguiente propiciar la caída del sistema, por esta razón se vuelve necesario indagar acerca del tema e identificar si existe una regulación concerniente al *double spending*.

## **2. OBJETIVOS**

### **2.1 Objetivo general**

- Caracterizar el fenómeno del *double spending* dentro del marco de funcionamiento de las criptomonedas a través de un proceso de análisis documental.

### **2.2 Objetivos específicos**

- Realizar un proceso de revisión bibliográfica sobre el *double spending* en el mercado de las criptomonedas.
- Establecer la dinámica de funcionamiento del *double spending* en el mercado de las criptomonedas.
- Identificar la regulación legal y normativa del *double spending* dentro del marco del funcionamiento de las criptomonedas.

## **3. JUSTIFICACIÓN**

La globalización ha incursionado en los últimos años de una manera trascendental en el diario vivir del hombre contemporáneo, abriendo espacios a nuevas tecnologías y dinámicas que traen consigo nuevos mercados y una mayor competitividad en los sectores

económicos, la forma tradicional de intercambiar bienes y servicios está quedando relegada y se empieza a utilizar herramientas más novedosas ya sea a través de la compra de cupones de descuento o puntos para canjear productos como modelo de fidelización de algunas compañías, el uso de nuevas unidades de intercambio o monedas electrónicas.

Un aspecto de gran importancia en este tema son las criptomonedas o monedas virtuales, las cuales permiten el intercambio de bienes y servicios a través de medios digitales sin la intervención de un tercero, cumplen aparentemente el mismo papel del dinero y expresan claras ventajas frente a otros mercados tradicionales, convirtiéndose en una gran competencia y amenaza para el sector financiero tradicional.

Las criptomonedas se pueden considerar un *boom* en este siglo por su alcance y magnitud, siendo utilizadas en diferentes compañías que las han acogido por sus beneficios, mencionadas en importantes series a nivel mundial e incluso aceptadas por muchas personas que han ingresado a este mundo.

El desarrollo de este tema tiene consecuencias relevantes para las políticas de cada país y repercute en las monedas tradicionales de los países, por eso ya se empieza hablar de ellas y toman cierta importancia en los planes de cada nación.

Se agrega que, pensar que alguna de las criptomonedas reemplazará las monedas soberanas de determinado país es improbable, pero si ya, algunas autoridades financieras a nivel internacional han decidido tomar acciones, significa que este nuevo sistema sí representa un escenario de cambio dinámico, significativo y trascendental, el cual es un foco de interés para el manejo y regulación de las nuevas economías mundiales.

A nivel internacional se ha venido trabajando para darle una regulación por su gran potencial a pesar de que no está totalmente claro el panorama, por el contrario, esta nueva

forma de intercambio de bienes y servicios ha sido poco estudiada y analizada en el ámbito nacional, sin garantías concisas y reglas claras a los interesados en incursionar en las criptomonedas, tanto el Banco de la República como la Superintendencia Financiera, se quedaron cortos al querer abordar el tema y dar sus respectivas posturas. Los enfoques de estas dos entidades no abren un espacio de discusión al tema, por el contrario, cierran un posible estudio y exploración de todos los aspectos en el mundo de las criptomonedas, es allí donde se hace necesario y urgente las investigaciones pertinentes.

Ahora bien, como un dato importante de este estudio investigativo se tiene que la cifra exacta de criptomonedas es muy difícil contemplarla porque tienen un crecimiento exhausto y esta cifra puede variar de un momento a otro, junto a ellas se han presentado desarrollos en obligaciones e instrumentos financieros.

El *Bitcoin* es la criptomoneda más importante hasta la fecha pues fue la primera que empezó a operar, más exactamente en el 2009 y desde ahí se ha mantenido en la cúspide, alcanzando un valor muy alto y siendo utilizada por un número significativo de personas y compañías. Esta moneda electrónica presenta características novedosas en cuanto a seguridad y facilidad de intercambio.

Además, se ha tratado de afirmar que se trata de una burbuja todo este sistema, que va tener su caída total en algún momento y que no va tener respaldo de nadie para ser salvada; sin embargo, el *Bitcoin* se ha recuperado de varias caídas anteriores y supone que han servido de aprendizaje para evitar recaer, parece que estas burbujas lo han fortalecido para crecer como unidad de valor.

Las criptomonedas se han posicionado como un gran atractivo para las empresas y personas naturales por sus beneficios, generando mayores ingresos por los bajos costos

operacionales de este sistema e incrementando la capacidad competitiva de las compañías, además, las criptomonedas pueden ser almacenadas en cualquier dispositivo y transferidos por la red global en cortos periodos de tiempo; sin embargo, también tiene sus riesgos que van desde la pérdida de monedas por ataques al sistema hasta la utilización en el lavado de dinero, también el problema del doble gasto, el cual es de suma importancia para el control de las operaciones en este tipo de moneda, por eso es necesario realizar un estudio que aborde este problema desde diferentes puntos de vista.

El problema del doble gasto o *double spending* permite que una unidad de valor sea gastada en dos operaciones a la vez, sin tener el suficiente valor para cubrir las dos operaciones por separado, es por esto que se considera un fraude al sistema el cual se debe controlar ya sea por los creadores o alguna autoridad.

Una posible solución es el sistema *Blockchain* ya que permite tener control de la información mediante registros seguros y sin alteración. “*Es un conjunto de tecnologías que combinadas hacen posible que computadoras y otros dispositivos puedan gestionar la información compartiendo un registro distribuido, descentralizado y sincronizado entre todos ellos, en vez de utilizar las tradicionales bases de datos*”. (López, 2017).

Este sistema debe ser abordado y explicado de manera detallada en el trabajo por su relación con el paradigma de las criptomonedas y el doble gasto.

Es necesario realizar una investigación sobre el problema del doble gasto en el mercado de las criptomonedas, abordando un análisis completo desde su caracterización hasta las posibles consecuencias y afectación a la economía del país. Este problema pone en alerta a los usuarios y autoridades y los obliga a estar atentos de este mercado y así evitar fraudes incontrolables a través de las criptomonedas.

La importancia de esta investigación radica en el aporte fundamental a la formación académica como estudiante del programa de Contaduría Pública, ya que este trabajo visualiza un problema que abarca la línea de las finanzas y permite tener claridad de unas posibles consecuencias en la economía sino se controla este doble gasto, así como un nuevo conocimiento de este tema tan relevante hoy en día.

#### **4. MARCO REFERENCIAL**

El dinero y los sistemas monetarios son precedidos, analizados y estudiados a través de diferentes enfoques y escuelas; según la escuela neoclásica el dinero es concebido como cualquier forma de cambio generalmente aceptado por todo el mundo a cambio de bienes y servicios. Desde esta perspectiva el dinero y el sistema monetario configuran cuatro funciones específicas:

1. Ser un medio de cambio: Cuando el dinero no existe los bienes deben ser intercambiados por medio del trueque, o sea, a través de un intercambio directo o de un servicio por otro, para lo cual, según los estudiosos debe existir una doble existencia de necesidad, lo cual tiene una estricta conceptualización capitalista ya que en este sentido el dinero cumple la función de separar las dos partes que intervienen en el trueque.
2. Ser un depósito de valor: Esta función alude a la capacidad que tiene el dinero de almacenar poder adquisitivo.
3. Ejercer como unidad de cuenta: Lo que significa que el dinero puede ser utilizado con fines contables sin necesidad de tener una existencia física, a través de los registros en los libros de contabilidad.

4. Actuar como patrón de pago de diferidos: Esta función está implícita en las nombradas anteriormente y hace alusión a que un pago debe hacerse hacia el futuro y pueda fijarse en términos monetarios, exactamente del mismo modo que pueda hacerse un pago el día de hoy. De esta manera, según esta concepción, el dinero actúa como una unidad de cuenta con una dimensión temporal adicional.

Otros estudios agregan que para que el dinero pueda ser concebido como dinero, en cualquiera de sus formas, debe cumplir con los siguientes requisitos:

- a. Ser aceptable.
- b. Ser portátil.
- c. Debe tener un alto valor en relación con su hecho divisible.
- d. Debe ser difícil de falsificar. (Viales, 2008).

Según este enfoque académico, el dinero y por consiguiente los sistemas monetarios han transitado en diversas etapas o fases. Un claro ejemplo de ello es como en la antigüedad, inicialmente la sal y el ganado en todas sus variedades (camellos, vacas, ovejas) cumplieron funciones de moneda. Sin embargo, es importante traer a colación que las primeras formas de moneda surgieron cinco mil años antes de la era actual, inicialmente estas tenían forma de bienes las cuales poseían un valor intrínseco; paulatinamente con la evolución comercial los historiadores argumentan que se consolidó una nueva etapa conocida como la etapa del dinero metálico, distribuida en tres periodos:

1. La moneda pesada: Surgió en Egipto 2000 años antes de la era actual, estas monedas tenían formas de lingotes, las cuales eran pesadas al momento de desarrollar las transacciones.

2. La moneda cuenta: fue creada 800 años antes de la era actual, cuando los lingotes comenzaron a ser divididos en pequeñas piezas, invento que fue instituido paulatinamente en países como Grecia, India, Roma y Arabia.

3. La moneda acuñada: en esta nueva modalidad o presentación de la moneda, estas todavía eran metálicas con la característica de que eran acuñada con algún símbolo o descripción, lo cual señalaba el peso de esta. Según estudios la fiabilidad de este último sistema de pagos está garantizado por el carácter perenne del metal; en esta fase el objetivo de este sistema monetario era garantizar la estabilidad de la moneda vs la arbitrariedad política impuestas por normas concernientes a la definición de su uso.

En estos sistemas monetarios cualquier metal podría ser usado; hubo un especial favoritismo por el uso de la plata y el oro; sin embargo, también se hizo uso de metales como el bronce y mixturas o aleaciones metálicas. También es importante recordar que las primeras monedas fueron elaboradas por las autoridades, a lo cual se imprimía un sello en cada una de ellas, la moneda como tal, fue empoderada en la época del medioevo, siendo acuñada directamente por los siervos del rey. Aunado a ello es importante recordar que desde esa época ya se cometían fraudes o estafas relacionadas al uso y creación de monedas.

También es importante agregar que debido a fenómenos como la inflación y los fraudes al sistema monetario, estudiosos de la economía crearon “la teoría cuantitativa del dinero y de los precios” según la cual “un cambio en la cantidad del dinero conduciría a un cambio en el nivel de precios en la misma dirección”, sumado a ello surge una teoría conocida como *la ley de Gresham* la cual estipula la existencia de un dinero malo o

fraudulento y de un dinero bueno o legal, según esta ley hay una tendencia a que el dinero malo busque reemplazar las monedas buenas. (Viales, 2008).

Ahora bien, existe también la aparición de una moneda nueva conocida como: “*el Cuasi- Dinero*” constituido por algunos activos que cumplían algunas funciones del dinero, en otras palabras, el cuasi dinero era un depósito de valor, que era fácilmente usable como medio de pago. El cuasi dinero da aparición a una figura contemporánea conocida como “*los depósitos a plazos*” o “*los sustitutos del dinero*”, los cuales son básicamente activos que pese a no ser medios de cambio pueden convertirse en ello, dichos en palabras de los teóricos, son elementos de cambio temporales pero sin ser depósitos de valor, lo cual da paso a su vez a una figura conocida como: “*la tarjeta de crédito*” la cual tiene su origen en Florencia, Italia en el siglo XVI. (Viales, 2008).

Quizás, una de las transformaciones en el sistema monetario más importantes fue la aparición del papel moneda el cual fue posicionado en el mundo a través de diferentes maneras, a diferencia de la moneda metálica elaborada en plata o en oro, el papel moneda no tiene un valor intrínseco, el papel moneda vale por lo que significa y no por lo que realmente es (a diferencia de una moneda elaborada en oro o en plata), es importante aclarar que el papel moneda también recibe el nombre de “*moneda fiduciaria*”, entendiendo que fiducia significa confianza en latín y hace alusión al hecho de que la gente confía en el valor que el papel moneda representa, no en lo que realmente es (solo papel impreso).

Según el historiador Manuel Chacón el papel moneda apareció como una forma para facilitar las transacciones, ya que las monedas metálicas eran muy pesadas, inicialmente las personas depositaban en los bancos una cantidad de dinero metálico y a cambio recibían el

papel moneda con el cual podrán realizar la compra práctica, sencilla y liviana de bienes o servicios.

Los primeros creadores del papel billete fueron los bancos chinos, posteriormente aparece la figura del “*papel moneda con recarga fraccionaria*” siendo respaldado por las reservas de los bancos y por el que se cobraba un interés con el que estos se enriquecían.

Posteriormente emergen figuras que institucionalizan nuevos sistemas monetarios o financieros, tales como la criptomoneda, la cual articula diferentes monedas de uso electrónico, la aparición de estas, están siendo un tema de gran interés e importancia a nivel nacional e internacional pero aún no se tiene claridad sobre ellas, por ese motivo es importante estudiarlas; algunos autores las definen de las siguientes maneras:

“Las monedas virtuales son una nueva medida contable, así como un medio de pago descentralizado sin intermediarios, que podría afectar a los hábitos de los consumidores así como el sector financiero” (Ordinas, 2017).

*“(...) Las criptomonedas son un nuevo concepto de dinero virtual, el cual fue desarrollado por primera vez en 1998 por Wei Dai en una lista de correo electrónico de criptografía, donde propuso la idea de un nuevo tipo de dinero que utilizara la criptografía para controlar su creación y las transacciones, en lugar de que lo hiciera una autoridad centralizada”. (Bargiela, 2016).*

Según (SCProgress, 2017) en la Revista de Comercio Electrónico:

*“(...) Una criptomoneda es una moneda virtual que sirve para intercambiar bienes y servicios a través de un sistema de transacciones electrónicas sin la necesidad de un intermediario. A diferencia de otros intentos de dinero electrónico,*

*las criptomonedas incorporan los principios de la criptografía para implementar una economía segura, anónima y descentralizada”.* (SCProgress, 2017).

Las criptomonedas son un avance para el mercado internacional y va aumentando de forma rápida con el paso de los días; sin embargo, este sector se vuelve una forma fácil para acceder a la ilegalidad, puesto que no se tiene un marco regulatorio que pueda controlar este sistema, su alta volatilidad se presta para incursionar en varios delitos, uno de ellos el lavado de activos.

Las criptomonedas son formas de inversiones y medios de pago consideradas de alto riesgo ya que su valor va ligado a la ley de la oferta y demanda. *“Bitcoin al ser una nueva tecnología y al ser una moneda que financieramente está regulada solamente por la ley de oferta y demanda, tiende a tener un alto grado de volatilidad.”* Generando así una relación evidente entre riesgo y rendimiento. (Caro y Obando, 2017).

*“(…) Según el Banco Central Europeo, las criptomonedas son monedas virtuales creadas y almacenadas en dispositivos electrónicos, pero no cuentan con ningún tipo de regulación en la mayoría de gobiernos, lo cual lleva a que se convierta en un mercado llamativo para invertir, pero con un margen de riesgo muy significativo”.* (Condusef, 2019).

Un dato sorprendente es que a la fecha la Real Academia Española no emite un concepto de la criptomoneda, lo que confirma la gran incertidumbre de este fenómeno.

Las criptomonedas están disponibles para ser aceptadas en el intercambio de bienes o servicios, así como en el pago de obligaciones y de esto depende el valor de las mismas, estando sujeta a la confianza que los usuarios tengan sobre ellas en el mercado y sobre la

opción de utilizarla en sus transacciones, si los partícipes dejan de usarlas y disminuyen las transacciones por consiguiente su valor va empezar a disminuir.

Las autoridades financieras en Colombia no pueden responder por una disminución significativa de un momento a otro en el valor de las criptomonedas ya que legalmente no son aceptadas como moneda de curso por el Banco de la República, además se menciona en otros partes del mundo el vínculo en operaciones ilícitas como lavado de dinero y fraude.

Según la página *web Coimarketcap*, el número de criptomonedas que existe a la fecha es de 2093, y las monedas virtuales más importantes de acuerdo con su capitalización son las siguientes: en primer lugar y sin discusión alguna se ubica el *Bitcoin*, con una capitalización de \$111.359.211.236, en segundo lugar el *Ethereum* con \$21.706.242.792 donde ya se evidencia una diferencia abismal comparada con el *Bitcoin*, en tercer puesto el *XRP* con un valor en su capitalización de \$20.311.730.893, en cuarto lugar el *Bitcoin Cash* con \$9.848.563.374 y por último en este ranking de las más sobresalientes se encuentra el *Stellar* con \$4.921.243.262. (Coinmarketcap, 2018).

Para tener una idea de estas importantes criptomonedas, se presenta una descripción de cada una de ellas: el *Ethereum*, es una moneda digital utilizada para realizar pagos a otras personas o a máquinas que ejecutan operaciones previamente solicitadas, esta plataforma permite realizar diferentes tipos de acuerdos de manera virtual. La identidad e información personal están bajo el control de la plataforma y tampoco depende de ninguna autoridad centralizada o entidad financiera. (*Ethereum*, 2018).

El *XRP (Ripple)* es de las más rechazadas dentro de las monedas virtuales, aunque es muy similar a otras monedas y usa los mismos protocolos, esta carece de un factor muy importante, la descentralización. La mayoría de los usuarios de esta plataforma son

instituciones bancarias, por lo que su argumento de descentralización no es confiable.

(*Ripple*, 2018).

*“(...) Bitcoin Cash trae dinero sólido al mundo, cumpliendo la promesa original de Bitcoin como "efectivo electrónico de igual a igual". Los comerciantes y los usuarios están habilitados con tarifas bajas y confirmaciones confiables. El futuro brilla intensamente con el crecimiento sin restricciones, la adopción global, la innovación sin permisos y el desarrollo descentralizado”. (Bitcoin Cash, 2018).*

“Por su parte, el *Stellar* es una plataforma que conecta bancos, sistemas de pagos y personas. Se integra para mover dinero de manera rápida, confiable y casi sin costo”.

(Tenorio, 2018). Esta criptomoneda trata de simular al *Bitcoin*; sin embargo, trata de añadir mejoras en su aplicación. Esta criptomoneda maneja una tecnología de código abierto para pagos y es un sistema perfecto para micro pagos y remesas en áreas donde el servicio bancario no es suficiente.

Ahora es mencionada la criptomoneda más importante en el mundo, el *Bitcoin*. El cual es un medio digital de intercambio de valor y tuvo su gran récord en cuanto a inversión en el año 2015. No depende de nadie, ni del gobierno, de ningún estado ni organismo centralizado. De la misma manera que cualquiera puede usar el correo electrónico, cualquiera puede usar *Bitcoin*.

### **El *Bitcoin*.**

*“El Bitcoin hará con los bancos lo que el correo electrónico hizo con la industria postal”*  
*Rick Falkvinge- Líder del partido Pirata de Suecia y de Microsoft.*

El *Bitcoin* es considerada la criptomoneda más importante desde su creación en el año 2009 por el pseudónimo de: “Satoshi Nakamoto”, del cual hasta el momento no se

conoce su verdadera identidad, desconociéndose si es una persona o un grupo de personas que se autoproclamaron bajo este alias.

En realidad, no es tan relevante conocer esta identidad sumado al hecho de que la tecnología de las *Bitcoins* funciona y en ella se puede depositar toda la confianza sin conocer su verdadero creador. Satoshi fue en busca de una moneda virtual descentralizada la cual incluyera una tecnología funcional que evitara fraudes y eliminara la existencia de terceros en las transacciones con la intención de reducir costos y además pudiese ser utilizada en el intercambio de bienes y servicios, siendo así cómo se creó el *Bitcoin*, cumpliendo con estas características e intereses iniciales.

Ahora bien, se conoce que el *Bitcoin* nació como una forma de rebelión a la solución que tuvo el gobierno americano de imprimir más dinero para solventar la crisis financiera, es allí donde Satoshi Nakamoto creó y publicó el *White Paper* (documento de 300 páginas en donde se explica el *Bitcoin* y su funcionamiento) con la intención de que este se convirtiera en la criptomoneda que reemplazaría el papel moneda y el medio de pago e intercambio más importante y confiable del mundo.

*“Sigo pensando en el Bitcoin. Hasta que no llegue a una conclusión, no lo apoyo ni lo rechazo. La gente también se mostró escéptica cuando el papel moneda reemplazó al oro”*

*Lloyd Blankfein-Director ejecutivo de Goldman Sachs y banquero estadounidense.*

Se define de la siguiente manera:

*“Bitcoin es una moneda digital criptográfica que usa tecnología P2P para operar sin necesidad de una autoridad central o bancos, creada por Satoshi Nakamoto en 2009. Bitcoin es de código abierto lo que significa que su diseño es público y todo el mundo puede ver el código fuente que sustenta la red”. (Martínez, 2014).*

La anterior definición es solo un abrebocas de este concepto, por eso se complementa con este significado: “*Bitcoin es la primera moneda descentralizada que utiliza el internet para enviar dinero directamente de persona a persona a cualquier parte del mundo las 24 horas sin tener que utilizar una entidad centralizada, un banco, PayPal o Western Unión*”. (Camargo, 2017).

Teniendo en cuenta muchos factores se puede afirmar que el *Bitcoin* es una moneda virtual descentralizada que puede utilizarse para realizar pagos, compras o diversas inversiones en los mercados nacionales e internacionales, sin la necesidad de terceros, estando en contravía de los procesos anárquicos del sector bancario tradicional.

La existencia y usabilidad de esta moneda puede apreciarse desde varios puntos de vista, según la oportunidad que vea la persona o empresa que la va a utilizar, ya sea en el intercambio de bienes y servicios, como medio de pago a sus trabajadores, o como una inversión para sacar provecho; algunos han llegado a creer que se pueden volver ricos con *Bitcoin*, pero esto no es más que un gravísimo error debido a la falta de información y la errada visión que tienen de este sistema monetario.

Por su parte, Hernando Fernández experto en materia y con un amplio recorrido en el tema llegando a ser minero en este mercado lo denomina “Oro 2.0” ya que, según él, *el Bitcoin* se convertirá en el reemplazo del oro por la fluctuación de su precio y tiene todos los elementos para ser una reserva de riqueza. Este investigador expresa el motivo por el cual lo considera así y son las siguientes características instituidas en este nuevo sistema monetario: convertible, movable, durable, divisible, seguro, limitado y descentralizado.

El objetivo de *Bitcoin* según su creador, quien usa el Pseudónimo de Satoshi Nakamoto (por la utilización de este seudónimo no se sabe si es una persona o un conjunto

de personas), es proveer una forma de intercambiar unidades de valor sin intermediarios que encarecen la operación como los bancos. En este sistema se puede asignar un apodo sin la necesidad de incorporar datos exactos para su identificación.

Nakamoto define la plataforma *Bitcoin* como “un sistema de pagos electrónicos basado en pruebas criptográficas en vez de confianza, permitiendo a dos partes interesadas realizar transacciones directamente sin la necesidad de un tercero confiable”. (Domínguez-Lúquez, 2018)

Domínguez y Lúquez (2018) definen *Bitcoin* como:

*“(...) Sistema que permite realizar transferencias confiables de dinero sin la necesidad de terceros o autoridades financieras pero en forma de una criptomoneda llamada Bitcoin, la principal novedad es su descentralización ya que son los mismos mineros quienes aseguran el funcionamiento correcto de las operaciones”.*

*Bitcoin* no es propiedad de nadie. Cualquiera puede usarlo, pero no hay una sola compañía que se encargue de ello. Las transacciones de *Bitcoins* son irreversibles, esto significa que nadie, ni los bancos ni los gobiernos pueden impedir enviar o recibir *Bitcoins*, en cualquier lugar del mundo. Con esta libertad viene la gran responsabilidad de no tener ninguna autoridad central por algún fraude o error. (*Bitcoin*, 2018).

*“Bitcoin* al ser un sistema descentralizado fija como límite la tasa de 21 millones de *Bitcoins*, cuando se llegue a esa cifra se espera que se detenga su emisión, actualmente se estima que hay en circulación 17'615.425”. (*Blockchain*, 2018).

Otro punto es el precio del *Bitcoin* que está sujeto a las leyes de la oferta y la demanda. Debido a que el suministro se limita a 21 millones de *Bitcoins*, cuando más personas usen *Bitcoin*, el aumento de la demanda, combinado con el suministro fijo, obligará

a que el precio suba. El mercado del *Bitcoin* es aun relativamente pequeño y por eso su precio puede variar cada día de manera significativa; sin embargo, su valor aumenta cuando más personas entran en el mercado y empiezan a realizar movimientos financieros. Por ejemplo, a principios de 2011, un *Bitcoin* valía menos que un dólar, pero en 2018 un *Bitcoin* ya vale cientos de USD. Si se cumplen los pronósticos para el futuro del *Bitcoin*, cada uno puede llegar a valer una cantidad exagerada de dólares. La organización *Bitcoin*, contempla varias formas de obtener esta moneda virtual: una de las más tentativas es aceptándolas como medio de pago de bienes o servicios. En la actualidad muchos establecimientos comerciales, físicos o digitales, aceptan esta moneda como medio de pago. Tal vez sea esta la forma más sencilla de obtener *Bitcoins*, solo basta brindar el código QR o la dirección del monedero digital al comprador para que realice la transacción, tanto el comprador como el vendedor del producto o prestador del servicio, deben tener claro la conversión de la moneda que manejan en *Bitcoins*. (Camargo, 2017).

Otras formas de adquirirlos son a través de una persona que los tenga y los quiera vender, realizando una transferencia electrónica internacional a una plataforma de intercambio (casa de cambio) para obtenerlos a través de *Localbitcoins*, donde los usuarios las compran y venden, a través de cajeros de punto de pago, o de intercambio internacionales como *Coinbase* o conseguirlos a través de la competitiva minería. (Camargo, 2017).

Existen varias formas de obtener *Bitcoin* como las mencionadas anteriormente, pero los intercambios de confianza son una de las mejores formas de adquirir *Bitcoin*. El sistema financiero cuenta con muchos déficits y es por esa razón que se tienen diferentes precios en los intercambios, es allí donde los comerciantes aprovechan la oportunidad para comprar a

un bajo precio y vender a un precio mayor. Cuando se presenta esta situación de precios tan variables es una alarma de que se presentan problemas y es necesario tomar medidas.

El *Bitcoin* trae consigo una serie de ventajas al momento de su uso, dependiendo de la óptica de cada usuario, entre las ventajas más importantes se encuentran las siguientes: la facilidad de pago del sistema, ya que con *Bitcoin* se puede enviar y recibir cualquier cantidad de dinero de manera inmediata sin importar el lugar del mundo donde se haga y en cualquier momento. No se tienen los inconvenientes de horarios de banco ya que la plataforma funciona todos los días del año las 24 horas.

Una de las principales ventajas son los costos más bajos frente al sector financiero, en la actualidad los pagos con *Bitcoin* se realizan con costos de transacción muy bajos e incluso gratis en algunos de ellos. Si un usuario desea que la transacción que acaba de realizar se procese con mayor rapidez, debe incluir un pago en su transacción. Servicios como tarjetas de crédito y Paypal entre otros que se utilizan como medio de pago, tienen altos costos por transacción en comparación con *Bitcoin*. Para las empresas y comerciantes los pagos con *Bitcoin* se depositan directamente en sus cuentas *Bitcoin*, las cuales son gratuitas de adquirir y manejar.

*“(...) Los riesgos bajos para los comerciantes ameritan ser mencionados como un plus del sistema, la seguridad, privacidad e irreversibilidad son algunos beneficios de los cuales gozan los comerciantes al utilizar Bitcoin. Al no contener información personal de los clientes las transacciones, el comerciante obtiene protección contra fraudes, disminuyendo de esta manera pérdidas. Adicionalmente Bitcoin da la posibilidad a estos comerciantes de vender sus productos en*

*mercados donde las tarjetas de crédito y servicios bancarios no se utilizan o las personas no pueden acceder a ellos. (Guzmán y Mesa, 2014).*

La seguridad con *Bitcoin* es una ventaja importante; los usuarios no asocian sus datos personales a las transacciones lo que les garantiza privacidad y los defiende contra un posible robo o suplantación de identidad, incluso tienen un total control sobre sus operaciones así nadie puede obligar un cargo sin la voluntad.

Una gran ventaja es que inicialmente el *Bitcoin* es imposible de falsificar o duplicar gracias a los algoritmos criptográficos, pese a ello, no se sabe hasta dónde pueden llegar quienes quieran poner en jaque este sistema. Ninguna cuenta de un usuario puede ser congelada ni tampoco intervenidas por alguna autoridad.

Por último, se encuentra la transparencia del sistema ya que las transacciones realizadas en la red *Bitcoin* pueden verificarse fácilmente a través de la cadena de bloque que está a la disposición de cualquier persona que quiera utilizarla para este fin. (Guzmán y Mesa, 2014).

Sin embargo, no todo es positivo, ya que el sistema también presenta algunas significativas desventajas que son mencionadas a continuación; el más importante es la volatilidad debido a que la cantidad de personas y negocios usando y aceptando *Bitcoin* es todavía muy pequeña comparado con el alcance que puede llegar a tener. Es por ello que eventos y noticias alteren los precios de *Bitcoin*. Teóricamente, la volatilidad será cada vez más pequeña en cuanto el uso del *Bitcoin* crezca y la tecnología en la cual está basada evolucione. (Guzmán y Mesa, 2014).

Esta moneda todavía cuenta con poca difusión a pesar de que cada día más negocios y empresas a nivel mundial aceptan y usan *Bitcoin* gracias a las ventajas que ofrece; estas son todavía un número pequeño.

*“(...) Una desventaja que no se puede pasar por alto es que el Bitcoin se encuentra en fase de constante desarrollo de nuevas herramientas y mejoramiento de la seguridad, así como completar algunas características que no se encuentran terminadas, por esta razón el sistema no brinda las garantías necesarias. Esta desventaja se debe a la fase de experimentación en que se encuentra esta moneda”.* (Guzmán y Mesa, 2014).

Un robo o ataque a las cuentas por parte de ciberdelincuentes es un miedo latente, ya que no hay posibilidad de recuperar lo que se han robado, solo por la propia voluntad de quien cometió el acto, lo que se cree poco probable. Esta desventaja debe ser la que más pone en vilo a los usuarios.

*“Sumado a ello se tiene que esta moneda emergente tiene algunos riesgos, el primero de ellos, y considerado también como desventaja es la volatilidad de la moneda, por lo cual los Bitcoins sufren alzas y bajas de su valor con mucha frecuencia, debido a que no dependen de ningún mercado y, por lo tanto, se puede considerar una moneda inestable. Ahora bien, por ser una moneda digital, la seguridad de la misma puede que sea una de las razones por las cuales fluctúa con tanta facilidad. Al presentarse ataques sobre cajeros de Bitcoins, monederos digitales o sobre las redes que resguardan los datos de los compradores y vendedores, incrementa la desconfianza sobre este instrumento de pago afectando su valor”.* (Cámara de Representantes Puerto Rico, 2018).

*“(…) Un segundo peligro está asociado a la ausencia de leyes regulatorias de este sistema. Por ser una moneda sin ningún tipo de regulación, la misma es utilizada con carácter particular. Es decir, para los usuarios no existe un ente regulatorio que proteja al consumidor, en caso de que se presente algún problema en las transacciones, no hay forma de colocar un reclamo o de ampararse en alguna ley. Para las empresas, el llevar a cabo transacciones con Bitcoins, está generando brechas importantes en su control interno, a causa de la mencionada ausencia de regulaciones, la consecuencia directa pudiese ser pérdidas que impacten directamente los estados financieros y la reputación o imagen de la empresa”.* (Aguilera, 2016).

*“(…) El último peligro a considerar es el blanqueo de dinero y mercado negro, ya que debido a la rapidez con que se realizan las transacciones, la falta de regulación, el anonimato, la cantidad de Bitcoins que existen hoy en día y el uso mundial, han hecho que esta moneda se vuelva muy llamativa para evasión de impuestos, lavado de dinero, evasión de control de cambio y cualquier transacción ilícita que se desee realizar”.* (Aguilera, 2016).

*“(…) La manera como se crean o generan Bitcoins es a través de la minería, este es un proceso mediante el cual un grupo de personas a través de computadores especializados contribuyen a la creación de Bitcoins, resolviendo problemas matemáticos complejos, que son fáciles de reproducir pero imposibles de revertir y difíciles de predecir, y como recompensa se reciben varias unidades de esta moneda”.* (Sarmiento, 2016).

En un principio cualquiera puede ser minero, aunque la realidad demuestra que son empresas que, como si de minas de oro se tratara, invierten gran cantidad de trabajo, esfuerzo y dinero en desenterrar los *Bitcoins*. Se necesita un gran poder computacional para ello, proporcionado por hardware especializado, de manera que los mineros con más poder o mayor eficiencia, serán los que tengan más posibilidades de desenterrar las nuevas monedas.

Un concepto muy importante para tener claridad del tema es el de monedero digital, el cual es el sitio virtual donde están registrados los *Bitcoins* que cada usuario posee en la red, este cumple la misma función de una billetera para el dinero en la forma física o análoga convencional; cada persona en este sistema posee un monedero digital identificado con una dirección, este se puede adquirir en las páginas oficiales de cada criptomoneda de manera rápida y gratuita en forma de *app* (aplicación virtual), solo con la descarga de esta a través del *app store* o *play store* de cada celular o dispositivo electrónico.

Para continuar, es pertinente explicar cómo se lleva a cabo el funcionamiento de una transacción en *Bitcoin*, lo primero que se debe tener para ello es un monedero virtual, este como ya se dijo anteriormente cumple la misma función de una billetera o una cuenta bancaria de cualquier país, con ello el usuario obtendrá una clave pública y una clave privada; la dirección como también es conocida, es visible para el resto de los partícipes en el mercado y la otra clave hará las funciones de la firma digital del usuario y sólo la conocerá el mismo.

Ahora bien, en el caso puntual de la realización de una transacción, se aclara que un usuario "X" puede contactar a un usuario "Y" a través de su dirección digital, teniendo la opción de hacer un envío de cualquier suma de dinero en *Bitcoins*, utilizando su firma digital (clave privada) para autorizar la transacción, una vez autorizada pasa a una cadena de

bloques (la misma tecnología *Blockchain*) en donde la función de los mineros entra en acción, siendo estos los encargados de validar las transacciones y recibir una bonificación en *Bitcoins* por su esfuerzo, después de validado todo el bloque de transacciones los *Bitcoins* estarán en la billetera digital del usuario “Y”; la confirmación por parte de los mineros tarda en promedio diez minutos y todas las transacciones son registradas en el sistema de contabilidad público descentralizado más conocido como “*Blockchain*” el cual será explicado en detalle durante el transcurso de este documento.

Dentro de todo este sistema ha surgido el problema de doble gasto, donde existe el riesgo de que la misma unidad de moneda digital se utilice en dos lugares es lo que en teoría sería el doble gasto, la forma más fácil para solucionarlo sería pensar en que uno de los pagos debe ser rechazado para evitar fraude pero esto conlleva un trabajo a fondo.

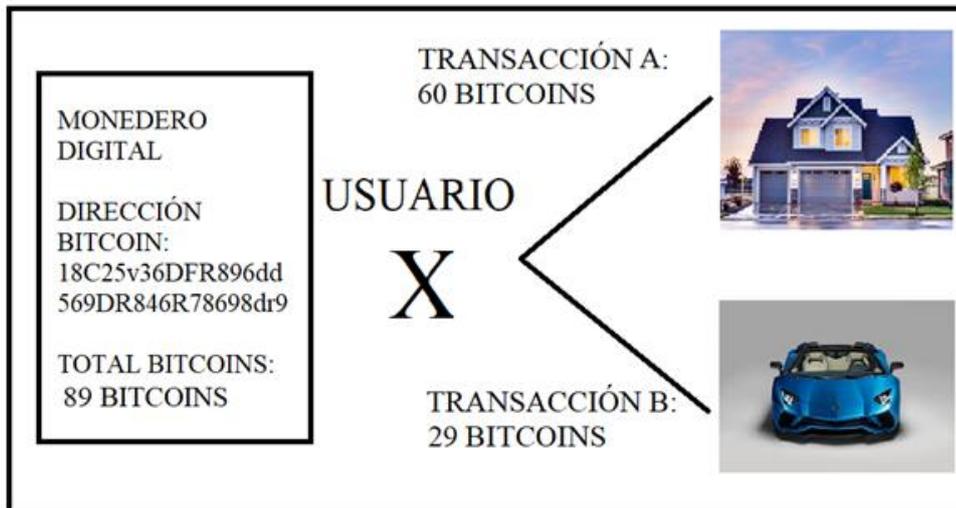
### **El fenómeno del *double spending* en el mercado de las criptomonedas**

El doble gasto o *double spending* es solo uno de los diversos problemas, fenomenologías, fallas o irregularidades, a los cuales están expuestas las criptomonedas, esta problemática no la tiene la moneda física-convencional, ya que al pagar en un tienda de ropa, restaurante o cualquier otro establecimiento con un billete, ese dinero ingresa a los fondos del local e inmediatamente el mesero, cajero o empleado devolverá el cambio, asegurándose de que ese billete entrante no es falso y que además cubre solo una transacción para el pago de los gastos requeridos por la compra o el servicio de manera total; a diferencia del dinero digital en donde sí se puede presentar este inconveniente ya que con frecuencia personas mal intencionadas intentan sacar provecho, tratando de cubrir los gastos por separado cuando en realidad solo tienen los fondos necesarios para cubrir una transacción, más no para efectuar exitosa y transparentemente las dos que se había propuesto inicialmente.

Para entrar en materia es inevitable citar dos definiciones que ayudan a esclarecer el tema, facilitando el ejercicio de comprensión sobre este tópico de interés:

*“El problema de doble gasto es una falla de los esquemas de dinero digital que consiste en que un solo token digital (moneda on-line) puede ser gastado dos veces. A diferencia del dinero físico como billetes y monedas, los archivos electrónicos pueden duplicarse y no evidenciar un cambio de titularidad (dueño) cuando es usado. (Castro, 2017).*

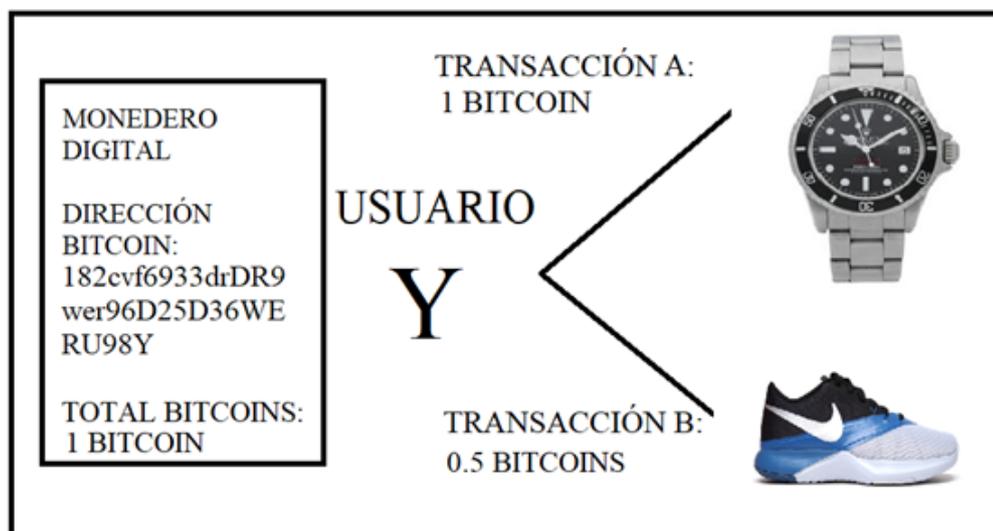
En otras palabras, Camargo define el doble gasto de la siguiente manera: *“es la posibilidad de que los Bitcoins sean gastados más de una vez por la misma persona”*. El *double spending* debe ser considerado como un fraude que debe tenerse en cuenta a la hora de involucrarse en el mundo de las criptomonedas y no solo del *Bitcoin*.



**Figura 1.** Perdomo, J. (2019) Transacción correcta de compra en *Bitcoins*. [Ilustración].  
Elaboración propia para los fines pertinentes de esta investigación.

En la anterior imagen se puede observar que el usuario X posee los fondos suficientes en su monedero digital para cubrir las dos transacciones por separado, en este caso no está intentando perpetrar un ataque de doble gasto, por lo tanto, la transacción será realizada exitosamente, sin incurrir en ningún delito o fraude; además de ello se agrega que

los montos económicos en *Bitcoins* dados en los ejemplos, corresponden a valores reales por los cuales se pagaría en la actualidad para la adquisición de uno de estos bienes.



**Figura 2.** Perdomo, J. (2019). Intento de doble gasto. [Ilustración]. Elaboración propia para los fines pertinentes de esta investigación.

En esta segunda imagen se evidencia cómo el usuario “Y” intenta cometer un ataque de doble gasto pues no tiene los fondos necesarios para cubrir las dos transacciones por separado, el total que necesita tener para las dos operaciones es de 1.5 *Bitcoins* y en su monedero digital solo posee 1, es decir, que solo puede cubrir una de las transacciones, esta persona busca de manera malintencionada realizar un fraude; sin embargo, los mineros a través de la tecnología *Blockchain* procuran actuar inmediatamente, deteniendo este acto de mala fe.

Es importante recordar que el doble gasto es una acción de carácter fraudulento o erróneo que consiste en enviar la misma criptomoneda a dos direcciones distintas, aprovechando que la primera transacción realizada aún no ha sido confirmada. Gracias a la tecnología *Blockchain*, este problema aplicable a las monedas digitales y al dinero electrónico es poco probable debido a la actividad realizada por los mineros de *Bitcoin*, que se encargan de confirmar y validar las transacciones, otorgándoles cadenas de bloques

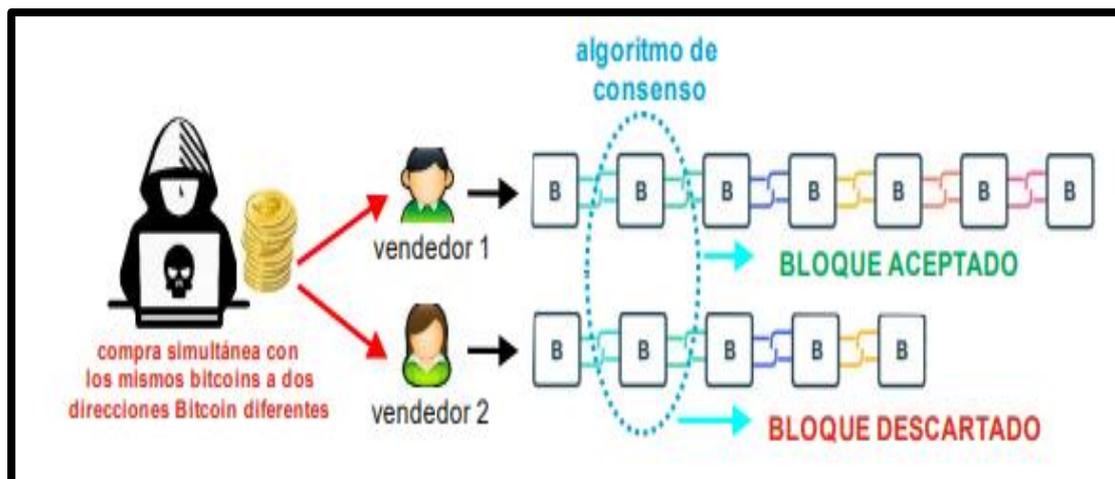
diferentes. Pese a ello, el sistema dista de ser perfecto y existen ciertos supuestos donde se podría dar esta situación.

Don y Alex Tappscot resumen el problema del doble gasto de la siguiente manera:

*“(...) Usted puede enviar la misma selfie a todos sus amigos, pero preferirá no darle a su amigo el dólar que ya le dio a alguien más. El dinero debe abandonar su cuenta y entrar a la de su amigo. No puede existir en dos lugares y mucho menos en múltiples lugares. Entonces hay un riesgo de gastar una unidad de moneda digital en dos lugares, de tal forma que uno de ellos rebote como un cheque sin fondos. Tradicionalmente, cuando se hacen pagos en línea, se soluciona el problema del doble gasto compensando cada transacción a través de registros centralizados de dos o más terceros”. (Castellanos, 2017).*

El doble gasto es un problema propenso para las criptomonedas por su facilidad para reproducir la información, cosa que no sucede con las monedas físicas, ya que no puede estar involucrada en dos transacciones al mismo tiempo.

De manera similar a la de las monedas físicas en donde se evita el doble gasto, sucede en un retiro de dinero en un cajero automático o en una entidad financiera, antes de que sea posible la operación el banco comprueba que efectivamente la persona cuente con la suficiente disposición de fondos y cuando ya se retire el dinero, el banco inmediatamente se encarga de ajustar el nuevo saldo de la cuenta, evitando de esa manera un ataque de doble gasto.



**Figura 3.** Lopez. R (2018). Posible ataque de doble gasto: Recuperado de: <http://openaccess.uoc.edu/webapps/o2/bitstream/10609/81739/7/blopezroTFM0618memoria.pdf>

Cuando una persona con intenciones fraudulentas intenta comprar ciertos productos simultáneamente a dos vendedores con los mismos *Bitcoins*, un minero mediante el algoritmo de consenso procesará y añadirá a la cadena de bloques solo una transacción, rechazando la otra, tal como se ilustra en la *figura 3*. De esta manera, si este usuario intenta realizar una transacción que ya utilizó esta nunca será incluida en el bloque y no existirá para el sistema, por tal motivo es muy importante el trabajo ágil y acertado de los mineros, el cual comienza con la labor de agrupar las transacciones en un bloque para verificar su validez, es decir, comprobar la procedencia de las monedas para garantizar que no son falsificadas o que no hayan sido gastadas con anterioridad. (Salinas, 2017).

El valor de las criptomonedas depende de la confianza que los partícipes de este mercado tengan sobre la calidad presente y futura de sus atributos para ser reconocidas y aceptadas como medio de pago, depósito de valor y unidad de cuenta frente a otras alternativas similares. Para generar esta confianza, estos esquemas deben garantizar que la oferta de las criptomonedas esté de alguna manera controlada, y que no pueda ser falsificada o utilizada por el mismo tenedor más de una vez (*the double spending problem*, o el

problema del gasto repetido o doble gasto); de tal manera que se preserve su valor adquisitivo.

### **Dinámica de funcionamiento del *double spending***

El usuario que quiera lograr exitosamente un ataque de doble gasto normalmente efectuar los siguientes pasos:

1. La persona empieza por seleccionar un servicio o producto de otra persona para realizar la transacción.
2. Posteriormente esta persona inicia el proceso normal de minar el bloque en el cual se encuentra la transacción correcta pero por otra parte genera un bloque engañoso, en donde el destino de las criptomonedas es la misma persona que comete el fraude.
3. Una vez se genera el bloque engañoso, la persona sigue minando el mismo hasta que tenga más confirmaciones que el bloque correcto, de esta manera consigue engañar al vendedor quien le prestará el servicio o le dará el producto al ver la transacción en el registro.
4. Si la persona realiza el paso anterior correctamente, el bloque falso será publicado y reconocido exitosamente, de esta manera la moneda gastada ingresará de nuevo a su monedero.

## **FORMAS DE CONTROLAR EL *DOUBLE SPENDING***

### ***Blockchain***

El *Blockchain* es una palabra desconocida para muchas personas hoy en día y por eso es determinante hacer referencia a este término:

*“El Blockchain o cadena de bloques es un registro público de transacciones que se mantiene mediante una red distribuida de computadores, que no requiere respaldo de ninguna autoridad central o una tercera parte y que ofrece un esquema transaccional libre de intermediarios, gracias al uso de algoritmos criptográficos. Sería como el libro de registros de contabilidad de una empresa en donde se registran todas las entradas y salidas de dinero, aunque en este caso hablamos de un libro de acontecimientos digitales que no requiere de un intermediario centralizado que identifique y certifique la información, sino que está distribuida en múltiples nodos independientes entre sí que la registran y la validan sin necesidad de que haya confianza entre ellos”.* (Castro, 2017).

El *Bitcoin* fue la primera criptomoneda en implementar esta tecnología *Blockchain* en su funcionamiento y en base a ello radica su gran éxito, ya que dentro de sus características más relevantes se encuentran su seguridad, confiabilidad y la reducción de costos y tiempos en las transacciones. Esta tecnología se puede ver reflejada no solo en las criptomonedas sino en muchos otros campos de acción como por ejemplo en el comercio, escuelas, hospitales, incluso los bancos ya han empezado a preocuparse por las amenazas que esta puede tener sobre su funcionamiento tradicional.

El *Blockchain* es una tecnología que está revolucionando todo este mercado pues Hernando Fernández afirma que funciona y garantiza una estabilidad en el sistema, incluso afirma que después del internet es la tecnología que mayor impacto tendrá, además cumple un papel determinante en este trabajo ya que controla el problema del doble gasto en un 100%, el cual es el tema de investigación en el presente, por esta razón no se puede pasar por alto.

Anteriormente se mencionó que el *Blockchain* soluciona este problema del doble gasto ya que cumple la misma función de *Visa* o *MasterCard* en las tarjetas de crédito convencionales, esta tecnología se encarga de validar si la persona posee los fondos necesarios para realizar las transacciones; Hernando Fernández en la entrevista afirma que el *Blockchain* soluciona en un 100% el *double spending*.

### **Prevención Centralizada**

Esta forma de prevenir el doble gasto es por medio de una tercera parte (persona o empresa) de total confianza que se encarga de validar que la moneda digital ha sido gastada en una transacción y no pretende cometer un fraude.

### **Prevención Descentralizada**

Bajo esta forma implementada por *Bitcoin* en 2009 se emplea un nuevo modelo criptográfico denominado prueba de trabajo (*proof-of-work*) evitando la necesidad de terceros que validen o confirmen la transacción, en esta modalidad se hace uso del *Blockchain* ya que las transacciones son guardadas en este libro de contabilidad pública.

Para solucionar este problema, Nakamoto creó una red que registra las transacciones en una cadena de bloques, denominada *Blockchain*.

*“(...) El Blockchain o cadena de bloques es un registro público de transacciones que se mantiene mediante una red distribuida de computadores, que no requiere respaldo de ninguna autoridad central o una tercera parte y que ofrece un esquema transaccional libre de intermediarios, gracias al uso de algoritmos criptográficos. Esta tecnología, que va más allá de las criptomonedas, promete transformar la forma en que se intercambia valor. La agilidad y seguridad al administrar la identidad de los actores en la red, rastrear los activos intercambiados*

*y la facilidad con la que se puede llevar a cabo el control y verificación de los contratos, plantea una disminución fundamental de costos y una reducción sustancial de la incertidumbre en las transacciones”.* (Castro, 2017).

En la tecnología *Blockchain* normalmente se crea un libro de contabilidad totalmente público donde se registran todas y cada una de las transacciones llevadas a cabo con la moneda. Son los propios usuarios los que se encargan de verificar las transacciones y aceptarlas como correctas, en el momento en que se confirma una transacción como correcta, ésta no puede ser cancelada. (Castro, 2017).

*“(…) El Blockchain configura el “Libro Contable Distribuido” (Distributed Ledger Technology), para anotar todos los pagos. Este registro o libro mayor, como también se le denomina, está custodiado en infinidad de ordenadores a lo largo y ancho de Internet, es decir, existen múltiples copias del mismo libro, cuyas páginas son firmadas digitalmente utilizando mecanismos criptográficos muy complejos que impiden cualquier tipo de alteración o manipulación de la información contenida en dichas páginas del Blockchain”.* (Rodríguez, 2014).

*“(…) La cadena de bloques consta de tres componentes fundamentales: transacciones, registro y un sistema que las verifica y almacena en bloques. Cada bloque se genera a través de un software que registra cronológicamente la información sobre cuándo y en qué secuencia han tenido lugar las transacciones, de allí deriva su nombre. Esta cadena ha funcionado de la mejor manera; sin embargo, no está exento de inconvenientes”.* (Castro, 2017).

*“(…) Esta tecnología permite que se realicen las transferencias electrónicas de una manera segura sin la presencia de un tercero de confianza y sin la necesidad*

*de la regulación financiera, dando solución a la principal barrera técnica de las últimas décadas para los desarrolladores tecnológicos, el problema del doble gasto*". (Castro, 2017).

Se aclara que, un usuario no puede reutilizar monedas que ya usó, puesto que la red rechazará la transacción porque éstas transacciones se hacen públicas, imposibilitando una reutilización, de hecho, en la página de *Blockchain* se puede observar casos de reutilización de monedas que se han detectado y bloqueado. (Herrera, 2016).

Desde la solución del problema de doble gasto, han aparecido numerosos competidores en el mercado, entre ellos se destacan: *Litecoin, Dogecoin, Mastercoin, Peercoin o Darkcoin*. Éstos simplemente cambian especificaciones técnicas, como el límite de la oferta monetaria, la velocidad de minado, los ajustes de dificultad o las recompensas.

Además, en el mercado de las criptomonedas se pueden presentar los siguientes ataques, los cuales según los autores son derivaciones del *double spending*:

### **Ataque de carrera**

Se presenta solo cuando los vendedores aceptan pagos sin confirmación (suceso que es poco probable) debido a que quedan expuestos a que la transacción sea restituida. Su nombre hace alusión a una carrera que se produce en el sistema para ver que transacción se acepta primero, es una competencia sin duda alguna.

### **Ataque Finney**

Este ataque al igual que otros es poco probable debido a que el vendedor debe aceptar transacciones no confirmadas, lo cual es inaudito por la inseguridad; además para llevar a cabo este fraude se requiere de un minero para que este devuelva las monedas a la

billetera digital. El atacante minero requiere tener controladas las dos direcciones involucradas en la transacción, él realiza la compra y él mismo acepta el pago, de inmediato bloquea la operación y las monedas las tendrá de nuevo en su monedero digital.

### **Ataque Vector 76**

Básicamente es una combinación de los dos ataques mencionados anteriormente, a diferencia de que se puede presentar en transacciones con una confirmación.

### **Ataque por fuerza bruta**

Este ataque depende de la potencia de procesamiento con la que cuente la persona que vaya a llevar a cabo este fraude, además necesita un gasto significativo de electricidad. En este proceso se hace una transacción y se paga al vendedor pero simultáneamente se crea una cadena de bloques alternativa, luego se debe esperar ciertas confirmaciones y de esta manera el vendedor intercambia el servicio o producto, seguido de esto se libera la cadena de bloques y el atacante tiene de nuevo su dinero en el monedero digital.

### **Ataque por mayoría o ataque >50%**

Es posible que se presente un ataque de doble gasto pero se conocerá como el ataque del 51% y esto quiere decir que más del 51% de los mineros se ponen de acuerdo para realizar un fraude al sistema, esto se puede decir que es casi imposible por la cantidad de mineros que deben ponerse de acuerdo en tan poco tiempo. Se necesita que esté bajo el poder de una sola persona u organización la mayoría del control para llevar a cabo esta maniobra lo cual es casi improbable hoy en día pero que igual da una luz de esperanza a las personas que siempre buscan el mal, por eso la afirmación de Hernando Fernández deja la inquietud de que el *Blockchain* soluciona 100% el problema del doble gasto. (Binance, 2019).

Si bien estos fraudes son difíciles de conseguir pero que al momento de que uno de estos personajes malintencionados logre su cometido podría poner en jaque el funcionamiento de cualquier criptomoneda, ya que su valor depende especialmente de la confianza que tengan los usuarios en las mismas y nadie va a querer entrar o seguir participando en un mercado que fue blanco de fraudes.

*“(…) Para lograr gastar una criptomoneda dos veces, el falsificador tendría que utilizarla para pagar a un comerciante y generar en secreto una cadena de bloques falsificada en la que no haya constancia de esa transacción. Al recibir la mercancía, el falsificador publicaría la cadena de bloques falsificada, es decir, anularía el pago. Sin embargo, esta cadena de bloques falsificada solo sería la cadena aceptada por la mayoría si fuera más larga que la cadena de bloques que el resto de la red de mineros produjo en forma paralela. Por consiguiente, para que un ataque de doble gasto (o fraude) tenga éxito, se requiere controlar un porcentaje significativo de la potencia computacional de la red minera, lo que es muy poco probable dado el actual tamaño de la red en el caso de Bitcoin, pero es un riesgo latente en el caso de las criptomonedas recientemente creadas”. (Universidad de los Andes, 2018).*

El *Bitcoin* maneja la aplicación denominada *peer to peer* (de igual a igual) la cual permite la comunicación entre las dos partes de la transacción sin tener que acudir a terceros, la relación es directa entre los interesados, evitando la interacción de otra persona que no esté en el negocio.

Se puede considerar que el *Blockchain* presenta unas ventajas tentativas y los bancos serían los más afectados, para lo cual deberán trabajar de la mano o esforzarse al máximo

por un sistema innovador que repliegue el mencionado. Por ejemplo, las instituciones financieras podrían reducir sus costos operativos si se implementa esta tecnología o una relacionada pero teniendo en cuenta su patente.

*“(…) A las entidades financieras y especialmente a los bancos centrales emisores de dinero, les provoca ansiedad y miedo a perder soberanía en el control de sus propias monedas, éste es el factor más importante que se considera sobre el aumento de restricciones legales. (Camargo, 2017). Pese a ello, Asobancaria estudia la posibilidad de adoptar la tecnología Blockchain, a sus procesos en los cuales las principales áreas en las que puede incursionar esta tecnología se destacan los medios de pago, los mercados de capitales e inversión y los procesos de cumplimiento, reflejado sin duda en una oferta de productos de ahorro, crédito e inversión más amplia y eficiente”. (Asobancaria, 2017).*

### **Panorama Local**

Entrando en materia legal referente al *Bitcoin* y el doble gasto del lado del gobierno colombiano, el Banco de la República emitió un comunicado de prensa en el cual ratificó como única moneda legal y en curso: “el peso colombiano”, advirtiendo que el *Bitcoin* no es una moneda colombiana y por lo tanto no existe la obligatoriedad de recibirlo en las transacciones diarias, esto sólo expresa el deseo de preservar una economía tradicional que siga girando en torno al peso colombiano, haciendo evidente el rechazo a la opción de que las criptomonedas entren en circulación en el mercado nacional colombiano.

La Superintendencia Financiera no está muy lejos de la posición del Banco de la República, expresando en circulares que las empresas bajo su supervisión no pueden entrar en este mercado y quienes lo hagan deben asumir por su cuenta las consecuencias al no estar

respaldadas por ninguna autoridad; esta postura no sorprende al tratarse de las dos autoridades máximas en materia económica del país, las cuales deben trabajar de la mano para sostener la estabilidad hegemónica en cuanto a este tópico de interés, además de la gran influencia que tiene el sector bancario para dar direccionalidad a diferentes instituciones, escenarios de poder y situaciones del país.

Articulado a ello, la DIAN hace énfasis en el proceso de la minería de *Bitcoins*, ya que los mineros reciben una bonificación por su trabajo, esto se traduce en ingresos que pueden formar parte del patrimonio del mismo y por tanto tener efectos en materia tributaria. Este organismo no es claro en cuanto al tema, pues no emite una circular específica donde exprese con exactitud y claridad sus criterios y apreciaciones referentes a la usabilidad y circulación nacional de las criptomonedas, así como tampoco genera una posible forma para presentarlas en la declaración de renta; lo que significa que una persona natural o jurídica puede ser propietaria de una suma millonaria de *Bitcoins* y no tener que rendir cuentas al estado por ello o pagar impuestos.

Según *Coinmap* (sitio web donde se encuentra el mapa mundial de los locales comerciales que aceptan *Bitcoins*), en Colombia existen aproximadamente 366 establecimientos de comercio que aceptan esta forma de moneda digital; en el caso de Neiva se estima que solo 5 lugares ya están en el mercado (Artista Bucheli, Ingeniero Kevin Sanchez, Obras de Arte Bucheli, Websalgusto.com y Bit-Card Colombia).

A la fecha se desconoce cuánto dinero han invertido los colombianos en *Bitcoins*, no existe documentación que de un registro detallado de esto ya que las criptomonedas hoy por hoy aún son un negocio incipiente, poco conocido y no cuenta con la total confiabilidad del

público colombiano lo cual ha de requerir un mayor tiempo para generar un proceso de empoderamiento y renombre dentro de la geografía nacional.

Por otra parte, según la revista Semana (2018), el mercado del *Bitcoin* es visto de buena manera solo por una parte de la población colombiana (no la totalidad); sin embargo, este fenómeno está creciendo a tal punto que ya las empresas empiezan a realizar talleres sobre el uso de la misma. Una de las causas por lo cual está creciendo este mercado es por los altos costos transaccionales del sector financiero tradicional, lo cual no es visto de buena manera en la mayoría de colombianos.

Es muy importante la unión de esfuerzos dentro de las empresas del sector financiero y de las TIC para alcanzar un avance significativo, además de la relación que ya existe de miembros de unos tipos de criptomonedas con los bancos.

### **Panorama Contable**

El último y más importante organismo que se ha pronunciado respecto al tema es el Consejo Técnico de la Contaduría Pública, por medio de los diferentes conceptos que suele emitir en su página *web*, siendo a través del concepto 472 del año 2018, en donde se afirmó que las criptomonedas no se pueden discriminar en ninguna categoría de activos en la actualidad y recomienda expresamente lo siguiente: *“Este consejo recomienda que se cree una unidad de cuenta separada para el reconocimiento, medición y revelación de transacciones y otros eventos o sucesos que tengan relación con las criptomonedas, que bien podría denominarse como “cripto-activos” o “activos virtuales”.* (Gaitán, 2018).

Hablar de las criptomonedas, especialmente el *Bitcoin* en materia contable es complejo, debido a la falta de información por parte de los máximos entes en materia, pero

sobre todo a la poca información existente traducida a la lengua castellana, ya que abundan textos en lengua inglesa, o en lenguas asiáticas (mandarín, chino y japonés).

Así mismo, esta moneda se vuelve un sistema muy llamativo debido a la incertidumbre y curiosidad de los altos rendimientos que puede llegar a proporcionar, cualquier persona o empresa estaría muy satisfecha con esas ganancias en dinero convencional; sin embargo, mientras que estas se encuentren en una página y no se pueda hacer uso de ellas de nada servirá. A la fecha dentro del panorama local aún existe una atmósfera de desconfianza respecto al hecho de invertir en este sistema financiero debido en gran parte a la misma forma como este se desarrolla.

Una persona natural que invierte en *Bitcoin* puede hacer la respectiva contabilización, pero solo al momento de la inversión y cuando recibe el dinero nuevamente, no puede realizar ajustes por los cambios abruptos que sufre la moneda mientras no reciba el dinero, solo hace los registros correspondientes por el principio de causación cuando recibe la utilidad; además la persona conoce las posibles consecuencias de entrar en el mercado y sabe que se pone en riesgo de perder este dinero de un momento a otro debido a la volatilidad de este sistema monetario, y a los ya mencionados ciberataques de las que son víctimas estas plataformas virtuales, sumado a ello como es claro, nadie se hará responsable de este hecho.

A continuación, para desarrollar mayor claridad sobre este tópico de interés, se ejemplifica un registro contable de una inversión de \$50.000.000 en criptomonedas, propiedad de una persona natural.

Tabla N. 1

*Registro contable de una inversión por persona natural*

<b>CÓDIGO</b>	<b>CUENTA</b>	<b>DÉBITO</b>	<b>CRÉDITO</b>
129995	Efectivo asignado a criptoactivos	50.000.000	
111005	Bancos Nacionales		50.000.000
<b>SUMAS IGUALES</b>		50.000.000	50.000.000

Nota. Perdomo. J. (2019). Registro contable de una inversión por persona natural. [Tabla]. Elaboración propia para los fines pertinentes de esta investigación.

Dentro de los siguientes 6 meses, esa inversión sufrió un ataque de doble gasto por 1 *Bitcoin* de valor equivalente a \$30.000.000, el registro de la pérdida en peso colombiano se hace de la siguiente manera:

Tabla N. 2

*Registro contable del dinero perdido por un ataque de doble gasto*

<b>CÓDIGO</b>	<b>CUENTA</b>	<b>DÉBITO</b>	<b>CRÉDITO</b>
129995	Efectivo asignado a criptoactivos		30.000.000
531595	Otros gastos extraordinarios	30.000.000	
<b>SUMAS IGUALES</b>		30.000.000	30.000.000

Nota. Perdomo. J. (2019). Registro contable del dinero perdido por un ataque de doble gasto. [Tabla]. Elaboración propia para los fines pertinentes de esta investigación.

Finalmente, esta persona natural decide retirar el dinero que quedó de su inversión después de sufrir este ataque y queda registrado de la siguiente manera:

Tabla N. 3  
*Registro contable del retiro de la inversión*

<b>CÓDIGO</b>	<b>CUENTA</b>	<b>DÉBITO</b>	<b>CRÉDITO</b>
129995	Efectivo asignado a criptoactivos		20.000.000
111005	Bancos Nacionales	20.000.000	
<b>SUMAS IGUALES</b>		20.000.000	20.000.000

Nota. Perdomo. J. (2019). Registro contable del retiro de la inversión. [Tabla]. Elaboración propia para los fines pertinentes de esta investigación.

### **REGULACIÓN LEGAL Y NORMATIVA DEL *DOUBLE SPENDING***

*“En sí mismo, el ejercicio del engaño no es especialmente fatigoso; es cuestión de experiencia, de práctica profesional”.*  
*"El espía que surgió del frío" 1963, John le Carré*

Como ya se ha dicho anteriormente la expansión y el conocimiento sobre criptomonedas, *Bitcoin* y doble gasto ha proliferado de manera vertiginosa, siendo así como en muchas latitudes del mundo ya es voz populi la circulación de estos conceptos; sin embargo, es pertinente decir que para la fecha las investigaciones en material bibliográfico y aun la información periodística que aborda los temas pertinentes a la regulación legal y normativa de las criptomonedas y el doble gasto es incipiente, novedosa y con frecuencia desarrollada en idiomas como el inglés o dialectos de origen asiático.

Es importante agregar que a inicios del año 2010 el plan de crear casas de cambio que posibilitaron la compra de *Bitcoins* por medio de transferencias bancarias ya era una realidad, posteriormente surgieron procesadores de pago que facilitaban el uso de *Bitcoins* mientras que las entidades encargadas de comercio cobraban el importe de ventas en sus cuentas bancarias haciendo uso de la moneda análoga tradicional de cada país, a este crecimiento exponencial se sumó que en el año 2015 surgió la incorporación de vehículos

financieros, los cuales posibilitaron escenarios para la compra de *Bitcoins* a través de “instituciones de inversión colectiva”.

A mitad del año 2015 fue inaugurado el *Bitcoin Investment Trust* (GBTC) en el *OTCQX Best Marketplace* en Estados Unidos de Norteamérica, lo cual dio la posibilidad a los inversores de cumplir las regulaciones financieras replicando el movimiento del precio del *Bitcoin* y también el *double spending* lo cual generó un escenario de mayor seguridad para aquellas personas naturales o jurídicas que entraban hacer uso de este nuevo sistema monetario. Sin embargo, esta forma de regulación no solo era nueva e incipiente, sino también insuficiente para el demandante diverso de usabilidad del *Bitcoin*, para el 2015 también se creó en Suecia el ETN *Bitcoin Tracker One*, el cual empoderaba la aparición y el uso de esta moneda en más de 178 países generando una forma de control y estabilidad necesaria para este sistema naciente.

En ese mismo año en Nueva York la casa de cambio *itBit Trust Company* regulada por las leyes bancarias de Estados Unidos se convirtió en la primera casa de cambio en *Bitcoins*, la cual operaba en completa armonía de acuerdo a las leyes estatales y federales del estado de Nueva York, generando además protección a través del FDIC para aquellas operaciones monetarias desarrolladas en Dólares.

Dentro del proceso pertinente de regulación de esta moneda, es importante agregar que en el año 2016 la *Financial Conduct Authority* del Reino Unido le brindó una licencia de dinero electrónico a la empresa *Circle* siendo la primera licencia entregada a una empresa compañía de *Bitcoin*, la cual además tenía un reconocimiento dentro de todo el marco del continente europeo.

En todo el sistema de empoderamiento y regulación de este nuevo sistema monetario también es valioso agregar que para el año 2016 en Estados Unidos fue aprobado el primer fondo de pensiones, el cual invertía *Bitcoins*, aprobando desgravaciones fiscales; el cual fue avalado por el *Internal Revenue Service*.

Así mismo, se debe agregar que las criptomonedas son un sistema financiero reciente, estructurado en una plataforma digital dinámica y constantemente cambiante, las formas de regulación en esta y de los atropellos que puedan suceder en ellas son también incipientes, pocos conocidos, medianamente comprendidos y divulgados, sumado al hecho de que todo ocurre dentro del contexto de la foraneidad, o sea, en el contexto extranjero, en donde predomina el uso de la lengua inglesa, o en idiomas propios del continente asiático, tales como el chino, el cantonés, el japonés o el mandarín; dentro de todo este escenario de novedad y cambios vertiginosos se puede concluir que el tema de la regulación tecnológica y legal de la figura del *double spending* requiere de un mayor tiempo para su desarrollo.

Por su parte, y como es apenas predecible el gobierno colombiano se encuentra muy relegado en cuanto a una posible regulación del tema de las criptomonedas en general y por consecuencia al doble gasto, a diferencia de otros países alrededor del mundo, como los que ya han sido nombrados con anterioridad en donde ya se empezó el proceso de control y regulación de la usabilidad de las criptomonedas y del doble gasto.

Se hace énfasis en que hasta el momento no se ha dicho mucho del tema y no hay leyes exactas que castiguen o penalicen a los practicantes del *double spending*, primero se debería pensar en una regulación del uso de las criptomonedas en el entorno colombiano, para posteriormente hablar de una regulación específica del doble gasto, en donde se establezcan medidas contundentes como sanciones económicas o judiciales para las

personas que logren cometer de manera exitosa este tipo de práctica cibernética delictiva, haciendo viable que con estas medidas el sistema financiero de las monedas digitales haga crecer de manera exponencial el número de participantes jurídicos o naturales que hacen parte de él.

También se debe considerar como una realidad fáctica que si el gobierno colombiano y en general los gobiernos internacionales no adoptan medidas de regulación y control, este escenario puede ser propicio para prácticas como la evasión de impuestos más grande de la historia y el lavado de dinero porque no existe un control donde se verifique la procedencia del mismo.

## **5. DISEÑO**

### **5.1 Clase de investigación.**

Al examinar los hechos y el planteamiento del problema ya expuesto con anterioridad; se ha determinado que el modelo de esta investigación es **no experimental**, de corte teórico-documental; por ello, es necesario desarrollar el ejercicio de recopilación documental relacionada con el problema del doble gasto, teniendo como referencia el enfoque de las criptomonedas, con opiniones que se limitan en el análisis de documentos con la problemática que se plantea.

### **5.2 Metodología de la investigación.**

El proceso de investigación se inicia con la recopilación documental del tema en cuestión, ya que son hechos de una actividad pasada, o en constante desarrollo; para lo cual se desarrollará el ejercicio de recopilación documental de informes, estudios, material audiovisual, archivos oficiales y periodísticos, posteriormente se analizará cada documento, además se aplicará una entrevista a una persona idónea en el manejo del tema la cual cumple

con ciertos requisitos específicos; sumado a ello, posteriormente se organizará la información seleccionada descartando aquella que no sea adecuadamente pertinente, para dar inicio a un proceso de escritura y caracterización del fenómeno del *double spending* en el mercado de las criptomonedas.

### ***5.2.1 Situación de la problemática.***

Se tiene en cuenta lo planteado en los antecedentes, en el cual se plantea el problema del doble gasto y la posible solución mediante el sistema del *Blockchain*.

### ***5.2.2 Modelo de análisis utilizado.***

El modelo de análisis elegido fue el descriptivo con el cual se busca sustentar los hechos y principales características del *double spending* en el mercado de las criptomonedas. Este análisis se basa en caracterizar el problema del doble gasto.

### ***5.2.3 Resultados.***

Después de utilizar el instrumento y estudiar los datos recolectados se espera caracterizar el *double spending* en el mercado de las criptomonedas. También se busca con esta indagación ampliar la información que se tiene relacionada a este tema.

## **5.3 Muestreo**

### ***5.3.1 Clases de muestreo***

Este proyecto es de tipo no probabilístico porque no es necesario que la muestra represente toda una población, se requiere realizar un estudio sobre una población específica mediante documentos.

### **5.3.2 Población**

Se tomarán en cuenta 10 documentos relacionados con el problema del doble gasto en las criptomonedas, donde estén consignadas características generales de este problema.

### **5.3.3 Muestra**

Se trabajará con 5 documentos que contengan características específicas para el cumplimiento del objetivo de la investigación y un adecuado análisis de la información, además se aplicará una entrevista a una persona en el tema.

## **5.4 Instrumentos para la recolección de datos.**

La recolección de datos será desarrollada a través de la recopilación documental y es necesario la realización de un formato que permita la obtención de los documentos ideales para un posterior ejercicio de análisis.

### **5.4.1 Herramientas para situación problema.**

El instrumento fue la recopilación documental relacionada con el problema del *double spending* y se toma como apoyo documentos de fuentes confiables.

### **5.4.2 Herramientas modelo análisis.**

Se utilizará herramientas para hacer análisis de la información relacionada al problema del *double spending* tales como la observación indirecta, la cual se caracteriza por desarrollar un ejercicio de revisión bibliográfica y/o video-gráfica, entendiendo que cada documento contiene características específicas que permiten caracterizar este problema; sumado a ello, también se desarrollará una entrevista abierta semiestructurada, la cual permite alcanzar información clara, oportuna y específica de una fuente confiable.

### 5.4.3 Resultados.

Al utilizar esta herramienta se obtienen resultados que permiten analizar el tema y de esa manera generar conclusiones sobre el objetivo planteado.

### 5.5 Recursos.

A continuación, se presentan expuestos los recursos con los que se llevará a cabo la presente investigación.

#### 5.5.1 Materiales de investigación.

Para la realización del proyecto de investigación se utilizarán los siguientes materiales.

Tabla N. 4  
*Materiales de investigación*

IMPRESIONES			INTERNET		
CANTIDAD	VALOR UNITARIO	VALOR TOTAL	HORAS	VALOR UNITARIO	VALOR TOTAL
300	200	\$60.000	200	1000	\$200.000
TOTAL DE GASTOS	\$260.000				

Nota. Perdomo. J. (2019). Materiales de investigación. [Tabla]. Elaboración propia para los fines pertinentes de esta investigación.

### 5.5.2 Recursos humanos.

Para desarrollar este proyecto se cuenta con la ayuda del director de la investigación, el docente Héctor Fernando Herrera Dussán.

Tabla N. 5  
*Recursos humanos*

DIRECTOR	VALOR TOTAL
Héctor Fernando Herrera Dussán.	\$500.000

Nota. Perdomo. J. (2019). Recursos humanos. [Tabla]. Elaboración propia para los fines pertinentes de esta investigación.

## 6. FINANCIACIÓN

El proyecto tiene un costo de \$760.000 (setecientos sesenta mil pesos) el cual estará financiado por el estudiante encargado del trabajo de grado.

Tabla N. 6  
*Financiación*

DATOS	VALOR
Materiales de investigación	\$260.000
Recursos humanos	\$500.000
Total	\$760.000

Nota. Perdomo. J. (2019). Financiación. [Tabla]. Elaboración propia para los fines pertinentes de esta investigación.

## 7. CRONOGRAMA

Tabla N. 7  
Cronograma

ACTIVIDAD/MES	1	2	3	4	5	6
Fundamentación teórica del proyecto.	X					
Búsqueda de referencia e indagación acerca del problema.		X				
Revisión de las fuentes primarias y secundarias.			X			
Aplicación entrevista			X			
Recolección de la información.				X		
Análisis de la información.				X		
Elaboración de informe final.					X	
Presentación y entrega del trabajo de grado.						X

Nota. Perdomo. J. (2019). Cronograma. [Tabla]. Elaboración propia para los fines pertinentes de esta investigación.

## 8. DATOS

Las siguientes tablas evidencian los datos obtenidos respecto al tema del doble gasto en los documentos seleccionados.

Tabla N. 8  
Documento N. 1

<b>ESTUDIO DE TECNOLOGÍAS BITCOIN Y BLOCKCHAIN</b>	
<b>Formas de control (<i>Blockchain</i>)</b>	El <i>Blockchain</i> resuelve el problema del doble gasto.
<b>Caracterización del fenómeno</b>	Un comprador actuando de mala fe, podría realizar dos compras simultáneas usando el mismo dinero.
<b>Dinámica de funcionamiento</b>	El doble gasto existe en el intercambio digital de dinero sin confirmación.
<b>Regulación legal y normativa</b>	Las operaciones en criptomonedas no están reguladas y por consiguiente el doble gasto no cuenta tampoco con un marco regulatorio estable.
<b>Panorama local</b>	No aborda el panorama local al tratarse de un documento foráneo.
<b>Ataques de doble gasto</b>	No existen datos respecto ataques de doble gasto.

Nota. Perdomo, J. (2019). Documento N. 1. [Tabla]. Elaboración propia para los fines pertinentes de esta investigación.

Tabla N. 9  
Documento N. 2

<b>CRIPTOMONEDAS, <i>BLOCKCHAIN</i> Y UNA NUEVA VISIÓN DEL MUNDO</b>	
<b>Formas de control (<i>Blockchain</i>)</b>	Nakamoto propuso una brillante solución alternativa al problema del doble gasto, sin necesidad de acudir a registros centralizados de terceros de confianza. ( <i>Blockchain</i> )
<b>Caracterización del fenómeno</b>	El doble gasto consiste en el riesgo de que se disponga de una unidad de moneda digital en dos lugares, de tal forma que uno de los pagos sea rechazado.
<b>Dinámica de funcionamiento</b>	Hay un riesgo de gastar una unidad de moneda digital en dos lugares, de tal forma que uno de ellos rebote como un cheque sin fondos.
<b>Regulación legal y normativa</b>	El Banco de la República demuestra la importancia de estos asuntos; reconoce su enorme potencial de transformación; y pone en evidencia las diferentes variables que debe considerar antes de adoptar alguna decisión regulatoria estructural.
<b>Panorama local</b>	El documento de origen local se limita abordar el tema de manera general, sin mayores datos locales.
<b>Ataques de doble gasto</b>	No existen datos respecto ataques de doble gasto.

Nota. Perdomo. J. (2019). Documento N. 2. [Tabla]. Elaboración propia para los fines pertinentes de esta investigación.

Tabla N. 10  
Documento N. 3

<b>CRIPTOACTIVOS</b>	
<b>Formas de control (<i>Blockchain</i>)</b>	No afirma que lo controla, pero sí aclara que en la tecnología <i>Blockchain</i> se lleva un registro de las transacciones lo que permite tener un control medido.
<b>Caracterización del fenómeno</b>	La criptomoneda no pueda ser falsificada o utilizada por el mismo tenedor más de una vez (the double spending problem, o el problema del gasto repetido o doble gasto); de tal manera que se preserve su valor adquisitivo.
<b>Dinámica de funcionamiento</b>	El documento aborda el contenido propuesto pero de manera superficial, adolece de elementos conceptuales y bibliográficos que poseen otros documentos.
<b>Regulación legal y normativa</b>	La regulación en el mundo se encuentra dividida, países en donde las apoyan por completo hasta naciones en donde están prohibidas totalmente, se agrega que este tópico de interés es aún novedoso y por consiguiente la bibliografía sobre el mismo es austera.
<b>Panorama local</b>	En Colombia los dos entes en materia prefieren preservar una economía estable que gire solo al peso colombiano, respecto al doble gasto no se menciona información normativa
<b>Ataques de doble gasto</b>	No existen datos respecto ataques de doble gasto.

Nota. Perdomo. J. (2019). Documento N. 3. [Tabla]. Elaboración propia para los fines pertinentes de esta investigación.

Tabla N. 11  
Documento N. 4

<b>¿TIENEN LAS CRIPTOMONEDAS LOS ATRIBUTOS NECESARIOS PARA REEMPLAZAR AL DINERO ACTUAL?</b>	
<b>Formas de control (<i>Blockchain</i>)</b>	Las criptomonedas superaron el problema del doble gasto a través de un registro descentralizado a través de lo que se conoce como un libro mayor distribuido. (Blockchain)
<b>Caracterización del fenómeno</b>	Cualquier forma de dinero digital es fácilmente replicable y, por lo tanto, se puede gastar fraudulentamente más de una vez
<b>Dinámica de funcionamiento</b>	Para que un ataque de doble gasto (o fraude) tenga éxito, se requiere controlar un porcentaje significativo de la potencia computacional de la red minera, lo que es muy poco probable dado el actual tamaño de la red en el caso de Bitcoin.
<b>Regulación legal y normativa</b>	La regulación legal y normativa no siempre se ajustan a las nuevas realidades como en el caso del nuevo mundo de las criptomonedas.
<b>Panorama local</b>	La Universidad de los Andes aborda este tema dentro del panorama local pero sin datos específicos y concretos.
<b>Ataques de doble gasto</b>	No existen datos respecto ataques de doble gasto.

Nota. Perdomo. J. (2019). Documento N. 4. [Tabla]. Elaboración propia para los fines pertinentes de esta investigación.

Tabla N. 12  
Documento N. 5

<b>BITCOIN, ¿REVOLUCIÓN O HISTORIA?</b>	
<b>Formas de control (<i>Blockchain</i>)</b>	La innovación tecnológica es el principal valor que ofrece Bitcoin, siendo la primera divisa digital que soluciona el problema del doble gasto para las transacciones a través de internet gracias a la tecnología Blockchain.
<b>Caracterización del fenómeno</b>	Un usuario malicioso intentará efectuar el doble gasto, esto es, realizar una transacción que es confirmada por la red y, posteriormente, con el mismo dinero realizar otra transacción.
<b>Dinámica de funcionamiento</b>	El doble gasto es propenso en el sistema digital de las monedas y solo podría ser posible si consigue un poder de computación del 51%.
<b>Regulación legal y normativa</b>	La regulación es uno de los grandes problemas de las criptomonedas, siendo poco claro cómo ha de ser gravado el concepto o como introducirlo en el marco legal. No se ha llegado aún a un consenso en referencia a estos aspectos.
<b>Panorama local</b>	No aborda el panorama local al tratarse de un documento foráneo.
<b>Ataques de doble gasto</b>	No existen datos respecto ataques de doble gasto.

Nota. Perdomo. J. (2019). Documento N. 5. [Tabla]. Elaboración propia para los fines pertinentes de esta investigación.

Tabla N. 13  
*Entrevista doble gasto*

<b>ENTREVISTA</b>	
<b>Formas de control (<i>Blockchain</i>)</b>	El <i>blockchain</i> soluciona en un 100% el problema del doble gasto.
<b>Caracterización del fenómeno</b>	Ataque al sistema de las criptomonedas al intentar cubrir dos transacciones cuando no tiene los fondos suficientes.
<b>Dinámica de funcionamiento</b>	Solo puede suceder en el dinero digital, no es posible en el dinero fiat.
<b>Regulación legal y normativa</b>	No conoce leyes exactas que castiguen a los autores de este delito.
<b>Panorama local</b>	No importa el lugar donde se presente un ataque de doble gasto, seguirá teniendo el mismo impacto pero las autoridades locales deben controlar esto.
<b>Ataques de doble gasto</b>	No conoce registros de ataques de doble gasto.

Nota. Perdomo. J. (2019). Entrevista doble gasto. [Tabla]. Elaboración propia para los fines pertinentes de esta investigación.

## 9. ANÁLISIS DE LOS DATOS

A continuación, y teniendo en cuenta las técnicas de análisis de información propuestas en el dispositivo metodológico de esta investigación se presentan las tablas que discriminan el proceso de observación indirecta o análisis documental pertinente a los textos seleccionados y estudiados para el desarrollo de este tópico de interés:

Tabla N. 14  
*Documentos seleccionados para el análisis documental*

<b>No. DOC</b>	<b>TÍTULO</b>	<b>AUTOR/ES</b>	<b>PAÍS</b>
1.	Estudio de tecnologías <i>Bitcoin</i> y <i>Blockchain</i>	Lopez, Benito	España
2.	Criptomonedas, <i>Blockchain</i> y una nueva visión del mundo	Castellanos, Erick	Colombia
3.	Criptoactivos	Arango, Carlos y Bernal, Joaquín	Colombia
4.	¿Tienen las criptomonedas los atributos necesarios para reemplazar al dinero actual?	Universidad de los Andes	Colombia
5.	<i>Bitcoin</i> , ¿revolución o historia?	Sanchez, Jaime	España
6.	Entrevista	Fernández, Hernando	Estados Unidos

Nota. Perdomo. J. (2019). Documentos seleccionados para el análisis documental. [Tabla]. Elaboración propia para los fines pertinentes de esta investigación.

A continuación, se presenta la tabla comparativa respecto al tópico de las formas de control (*Blockchain*) desarrolladas para regular el ataque del *double spending* en la web:

Tabla N. 15  
*Formas de Control sobre el Double Spending*

<b>No.</b>	<b>¿El documento identifica las formas de control del <i>double spending/Blockchain</i>?</b>
<b>Doc. 1</b>	Si, el documento aborda dentro de su contenido el protocolo <i>Bitcoin</i> sobre la tecnología <i>Blockchain</i> , identificando el problema del doble gasto como un escenario desarrollado por delincuentes cibernéticos.
<b>Doc. 2</b>	Si, el documento aclara que Satoshi Nakamoto resolvió este problema basado en la tecnología <i>Blockchain</i> , aclarando que esta es eficiente en la labor de evitar esta clase de prácticas criminales.
<b>Doc. 3</b>	No afirma que lo soluciona, pero sí aclara que en la tecnología <i>Blockchain</i> se lleva un registro de las transacciones lo que permite tener un control medido; el documento no desarrolla a profundidad este tema y deja algunas dudas y cuestionamientos al respecto.
<b>Doc. 4</b>	Si, este documento aborda este tópico de interés, agregando que las criptomonedas superaron el problema del doble gasto a través de un registro descentralizado, lo que también se conoce con el nombre de tecnología <i>Blockchain</i> .
<b>Doc. 5</b>	Si, este documento aclara que el principio para solucionar todo tipo de ataque criminal está instituido en la innovación electrónica, lo que a su vez puede resolver y regular fenomenologías criminales como la del doble gasto. Sumado a ello, el texto da un concepto favorable a la tecnología de bloqueo criminal identificada como <i>Blockchain</i> declarando que esta es innovadora, efectiva y confiable.
<b>Ent.</b>	El problema del doble gasto es solucionado en un 100% por la tecnología <i>Blockchain</i> .

Nota. Perdomo. J. (2019). Formas de control. [Tabla]. Elaboración propia para los fines pertinentes de esta investigación.

Ahora bien, respecto al tópico de interés, interesado en caracterizar, definir o describir la figura del *double spending*, el ejercicio de análisis documental encontró lo siguiente (Ver tabla 16):

Tabla N. 16  
*Caracterización del Double Spending*

<b>No.</b>	<b>¿Caracteriza el fenómeno del <i>double spending</i> dentro del mercado de las criptomonedas?</b>
<b>Doc. 1</b>	Si, este documento realiza aportes significativos a la definición conceptual del fenómeno del <i>double spending</i> , aclarando que esta es una dinámica por la cual un comprador actuando de mala fe intenta realizar dos compras simultáneas usando el mismo dinero.
<b>Doc. 2</b>	Si, este documento desarrolla un trabajo de caracterización de esta tecnología, sumado a ello identifica y caracteriza el <i>double spending</i> como un riesgo financiero cibernético desarrollado por expertos cibercriminales.
<b>Doc. 3</b>	Si, el texto es enfático al afirmar que la criptomoneda puede ser falsificada o utilizada por el tenedor más de una vez; sin embargo, este escenario no es muy frecuente y tampoco está penalizado por la ley.
<b>Doc. 4</b>	Si, el texto desarrolla un ejercicio de caracterización del <i>double spending</i> , aclarando que la criptomoneda al ser dinero digital es fácilmente replicable y se puede gastar fraudulentamente más de una vez.
<b>Doc. 5</b>	Si, el texto aborda superficialmente este eje temático, argumentando que es la posibilidad de que el dinero se utilice dos veces sobre plataformas digitales, configurando una escena de crimen cibernético- <i>on line</i> .
<b>Ent.</b>	Si, expresa que un usuario posee un <i>Bitcoin</i> en la billetera y trata de gastarlo dos veces en dos transacciones diferentes, tratando de enviar el mismo <i>Bitcoin</i> a dos billeteras separadas, no tiene los fondos suficientes para cubrir las dos transacciones.

Nota. Perdomo. J. (2019). Caracterización del *double spending*. [Tabla]. Elaboración propia para los fines pertinentes de esta investigación.

Sumado a ello, respecto a la dinámica de trabajo del *double spending*, el ejercicio de revisión documental halló lo siguiente: (Ver tabla 17)

Tabla N. 17  
*Funcionamiento del Double Spending*

<b>No.</b>	<b>Define la dinámica de funcionamiento del <i>double spending</i> en el mercado de las criptomonedas.</b>
<b>Doc. 1</b>	Este texto argumenta que el funcionamiento del <i>double spending</i> se basa en el intercambio del dinero digital sin confirmación, este intercambio se da por bienes o servicios; agregando que para ello se efectúa un proceso riguroso a través del cual se efectúa esta práctica delictiva.
<b>Doc. 2</b>	Este documento aclara cómo es la dinámica de funcionamiento del <i>double spending</i> ; a lo cual agrega que esta se basa en que la moneda digital no puede existir en dos lugares diferentes, solo puede cubrir una transacción; cuando cubre más de una es cuando se configura el delito del doble gasto.
<b>Doc. 3</b>	No, el documento aborda el contenido propuesto pero de manera superficial, adolece de elementos conceptuales y bibliográficos que poseen otros documentos.
<b>Doc. 4</b>	Este documento aclara respecto a la dinámica de funcionamiento del <i>double spending</i> que cada usuario de la red almacena una copia actualizada de todo el libro (esto es lo que lo hace "distribuido"). Con un libro mayor distribuido, el intercambio de dinero digital entre pares es factible, ya que cada usuario puede verificar directamente en su copia del libro contable si se realizó una transferencia y si no hubo intento de realizar un doble gasto.
<b>Doc. 5</b>	Una vez se efectúa una transacción, ésta es distribuida por todos los nodos de la red para su confirmación y colocación en un bloque. La firma permite que la operación no sea alterada durante este proceso y la cadena de bloques y minería previene el doble gasto, sin embargo, la información precisada por este documento se queda corta comparada con otros textos.
<b>Ent.</b>	El problema del doble gasto no se puede presentar en el dinero físico, solo puede ser posible en el dinero digital por la duplicación de archivos.

Nota. Perdomo. J. (2019). Funcionamiento del *double spending*. [Tabla]. Elaboración propia para los fines pertinentes de esta investigación.

Respecto a el t3pico de la regulaci3n legal y normativa abordada para regular el *double spending* dentro del marco de las criptomonedas, los diferentes autores sustentan lo siguiente: (Ver tabla N. 18)

Tabla N. 18  
Regulaci3n Legal y Normativa

<b>No.</b>	<b>Identifica la regulaci3n legal y normativa del <i>double spending</i> dentro del marco de funcionamiento de las criptomonedas.</b>
<b>Doc. 1</b>	Respecto a este t3pico de inter3s, el documento argumenta que las operaciones en criptomonedas no est3n reguladas y para el <i>double spending</i> no existe normativa que pueda sancionar de manera puntual y contundente a los autores de esta clase de estafas digitales.
<b>Doc. 2</b>	El Banco de la Rep3blica demuestra la importancia de estos asuntos; reconoce su enorme potencial de transformaci3n; y pone en evidencia las diferentes variables que debe considerar antes de adoptar alguna decisi3n regulatoria estructural. Siempre se debe tener presente el fomento de la innovaci3n.
<b>Doc. 3</b>	La regulaci3n en el mundo se encuentra dividida y en Colombia los dos entes en materia prefieren preservar una econom3a estable que gire solo al peso colombiano, respecto al doble gasto no se menciona informaci3n normativa; se agrega que este t3pico de inter3s es a3n novedoso y por consiguiente la bibliograf3a sobre el mismo es austera.
<b>Doc. 4</b>	El dise1o y la implantaci3n efectiva de la normativa no est3n exentos de dificultades. Las definiciones jur3dicas y reguladoras no siempre se ajustan a las nuevas realidades como en el caso del nuevo mundo de las criptomonedas.
<b>Doc. 5</b>	La regulaci3n es uno de los grandes problemas de las criptomonedas, siendo poco claro c3mo ha de ser gravado el concepto o como introducirlo en el marco legal. No se ha llegado a3n a un consenso en referencia a estos aspectos.
<b>Ent.</b>	No conoce leyes exactas que sancionen esta pr3ctica.

Nota. Perdomo, J. (2019). Regulaci3n legal y normativa. [Tabla]. Elaboraci3n propia para los fines pertinentes de esta investigaci3n.

En lo pertinente a cuál ha sido el desarrollo del panorama local de la figura del *double spending* se presenta la tabla N. 19:

Tabla N. 19  
*Panorama Local del Double Spending*

<b>No.</b>	<b>Aborda el panorama local del <i>double spending</i>.</b>
<b>Doc. 1</b>	El documento no hace mención sobre el panorama local del <i>double spending</i> al tratarse de un documento de otro país; sin embargo, tampoco aborda o estudia el caso de esta fenomenología dentro del contexto mundial, genera escasamente algunos comentarios sobre el mismo, definiéndolo como una problemática incipiente pero real.
<b>Doc. 2</b>	El documento de origen local se limita abordar el tema de manera general, sin mayores datos locales.
<b>Doc. 3</b>	El Banco de la República y la Superintendencia Financiera ya tienen conocimiento del tema y por tanto emite su significado.
<b>Doc. 4</b>	La Universidad de los Andes aborda este tema dentro del panorama local; especificando que el problema del doble gasto es una fenomenología que genera pérdidas significativas, no solo en el sector local sino también en la esfera global.
<b>Doc. 5</b>	No hace mención del panorama local del <i>double spending</i> al tratarse de un documento de otro país.
<b>Ent.</b>	Se debe trabajar en el panorama local para adoptar las criptomonedas y posteriormente el doble gasto.

Nota. Perdomo, J. (2019). Panorama local. [Tabla]. Elaboración propia para los fines pertinentes de esta investigación.

Los diferentes autores expresan lo siguiente respecto a los ataques de doble gasto que se han presentado. (Ver tabla 20)

Tabla N. 20  
*Ataques de Doble Gasto en Colombia*

No.	¿Dentro del panorama colombiano se han presentado ataques de doble gasto?
<b>Doc. 1</b>	El documento no hace mención de este dato.
<b>Doc. 2</b>	El documento no hace mención de este dato.
<b>Doc. 3</b>	El documento no hace mención de este dato.
<b>Doc. 4</b>	El documento no hace mención de este dato.
<b>Doc. 5</b>	El documento no hace mención de este dato.
<b>Ent.</b>	No tiene conocimiento de ataques de doble gasto.

Nota. Perdomo. J. (2019). Ataques de doble gasto. [Tabla]. Elaboración propia para los fines pertinentes de esta investigación.

## 10. RESULTADOS Y CONCLUSIONES

Respecto al tema de las criptomonedas y de manera específica al *Bitcoin*, este ejercicio investigativo académico concluye que este nuevo sistema monetario en efecto si está revolucionando de manera exponencial el panorama económico a nivel mundial, propiciando un cambio de paradigma en cuanto a la visión del dinero convencional, los escenarios económicos y las formas de comercialización vigentes, llevando a las naciones a tomar medidas progresivas y estandarizadas en cuanto a este tema, las cuales están direccionadas a reconocer e identificar las consecuencias de la usabilidad de este incipiente sistema monetario.

De igual forma se concluye que el *Bitcoin* es la criptomoneda más reconocida e importante a nivel mundial (por encima de otras como el Ethereum, XRP, Bitcoin Cash,

Stellar), siendo utilizada en el intercambio de bienes y servicios a través de personas naturales y/o jurídicas, en casas de cambio y para invertir a corto, mediano y a largo plazo. Es de agregar que para el funcionamiento de esta moneda digital, es importante el trabajo de los mineros digitales, quienes validan las transacciones y permiten un comportamiento estable de la plataforma, los usuarios se conectan directamente para intercambiar bienes o servicios por una cantidad determinada de *Bitcoins*.

Los estudiosos del tema coinciden en afirmar que la estructura de protección, control y/o regulación del *Bitcoin* se encuentra basada en la tecnología *Blockchain*, la cual potencializa el uso de este sistema monetario, estructurándolo sobre un significativo y eficiente estándar de seguridad; sin embargo, se aclara que este no es absolutamente confiable, ya que es pertinente traer a colación las diferentes ocasiones en las que se han presentado situaciones de robo o fraude a través de prácticas cibernéticas similares al *double spending* o doble gasto, el cual es definido por expertos financieros como un tipo de fraude digital o ataque al sistema *on line* de las criptomonedas. Esta práctica generalmente ocurre cuando un usuario o ciber criminal, intenta realizar dos transacciones por una determinada suma de *Bitcoins*, teniendo la cantidad disponible solo para una transacción o pago, para ello el atacante debe contar con el suficiente poder computacional para poder generar un bloque falso y minarlo, esperando hasta recibir la mayor cantidad de confirmaciones del bloque verdadero, lo que posibilita que el vendedor libere el producto, luego de validar estas confirmaciones y verificar la procedencia “aparentemente correcta” de los *Bitcoins*; sin embargo, como es bien sabido, los *Bitcoins* nunca ingresaran al monedero digital del vendedor, consolidándose de esta manera un ataque de doble gasto; esto se propicia debido a que los archivos digitales son fácilmente replicables en la red. También es importante agregar que este problema nunca sucedería con el dinero físico convencional.

Los autores argumentan de diferentes maneras contenidos que identifican como un fraude al sistema, el hecho de utilizar la misma criptomoneda en dos transacciones diferentes, siendo enfáticos en definir esta actividad como *double spending*. Se puede inferir que el funcionamiento del doble gasto en el mercado de las criptomonedas sería propenso por su duplicación en el sistema *on line*, situación que es argumentada por las investigaciones abordadas.

Respecto a las formas de prevenir esta situación problemática, se aclara que esta se hace a través de una entidad centralizada, la cual controla las transacciones y todos los movimientos financieros o utilizando el sistema descentralizado conocido como *Blockchain*, el cual es el más utilizado en el universo financiero de las criptomonedas y especialmente en el del *Bitcoin*. Sumado a ello, todos los autores coinciden en afirmar que la tecnología *Blockchain* controla el problema del doble gasto, argumentando que esta es eficiente y confiable.

En lo pertinente a las conclusiones articuladas al panorama contable de las criptomonedas, se precisa que aún se vislumbra falta de claridad y precisión, ya que a la fecha el escenario de desarrollo interactivo y económico del *Bitcoin* y del *double spending* no es del todo entendido y tampoco es fácil de rastrear; pese a ello los profesionales en contabilidad han empezado un proceso de acercamiento, comprensión y apropiación de este universo económico, desarrollando empatía académica e investigativa hacia este tema, por medio de los conceptos que emite el Consejo Técnico de la Contaduría Pública (CTCP).

El *double spending*, en términos generales no puede ser contabilizado, tampoco existen cifras publicadas de cuánto dinero ha sido hurtado a través de esta figura dentro del

contexto local, nacional o mundial; sin embargo, debe ser tenido en cuenta para no conducir a un posible escenario de liquidación de empresas que sufran ataques de este tipo.

Se confirma que es casi improbable hablar en materia legal y normativa que aborde el crimen o fraude del *double spending*, debido a que este es aún una figura nova e incipiente, y apenas se viene trabajando en las primeras propuestas de regulación en algunos países donde ya está funcionando el mercado de las criptomonedas.

Aún a la fecha es poco probable hablar de una regulación o un control legal y normativo dentro del panorama local e internacional concerniente a la figura del *double spending* en el marco del mercado de las criptomonedas, debido a que no se ha regulado y reconocido formalmente este sistema monetario; siendo así como a la fecha en ningún país se ha creado una norma o ley que aborde, sancione o penalice de alguna forma el crimen del *double spending*, ya que como se dijo al interior del documento ni siquiera se han creado instrumentos de reconocimiento y regulación de las criptomonedas como sistema monetario pero a grandes rasgos se debe hacer hincapié en la creación de un sistema de control y regulación urgente para estos dos tópicos, evitando que avance a tal punto que no se puedan controlar y se llegue a instancias tales como la transformación de este sistema en un espacio propicio para la ilegalidad, la evasión de impuestos, el lavado de dinero y otras formas de fraudes económicos.

De igual forma al realizar el análisis documental se halló que no existen registros en el panorama colombiano que daten de ataques de *double spending*, esto se debe en gran medida a que esta forma de sistema monetario es nuevo y poco conocido y estudiado en las latitudes nacionales.

## BIBLIOGRAFÍA

- Aguilera, V. (2016). Bitcoin: conoce sus características y riesgos, Economía, El Estímulo, Venezuela, recuperado de: <http://elestimulo.com/blog/bitcoin-conoce-sus-caracteristicas-y-riesgos/>.
- Arango, C.; Barrera, M.; Bernal, J.; Boada, A. (2018). Criptoactivos, Colombia: Banco de la República, recuperado de: [http://www.banrep.gov.co/docum/Lectura\\_finanzas/pdf/documento-tecnico-criptomonedas.pdf](http://www.banrep.gov.co/docum/Lectura_finanzas/pdf/documento-tecnico-criptomonedas.pdf)
- Banco de la República. (2014). Comunicado Bitcoin, Colombia, Bogotá, recuperado de: <http://www.banrep.gov.co/es/comunicado-01-04-2014>.
- Bargiela, J. (2016). Criptomonedas, Buenos Aires.
- Binance, A. (2019). Dusting Attack, artículo, recuperado de: <https://www.binance.vision/es/security/what-is-a-51-percent-attack>
- Bitcoin. (2018). Cosas que necesitas saber, recuperado de <https://www.bitcoin.com/>
- Bitcoin Cash (2018). La mejor moneda del mundo, recuperado de <https://www.bitcoincash.org/>
- Blockchain. (2018). Bitcoins in circulation, recuperado de: <https://www.blockchain.com/es/charts/total-bitcoins>).
- Cabrera, F. (2018). Tecnología Blockchain: elementos básicos, aplicaciones y marcos regulatorios, Chile: Biblioteca del Congreso Nacional de Chile.
- Cámara de Comercio de Bogotá. (2018). Entendiendo los criptoactivos, Colombia, Bogotá, recuperado de: <https://bibliotecadigital.ccb.org.co/bitstream/handle/11520/22729/5/20Entiendo%20los%20cripto%20activos.pdf?sequence=1&isAllowed=y.2018>
- Cámara de Representantes Puerto Rico. (2018). Puerto Rico, recuperado de: <http://www.tucamarapr.org/dnncamara/Documents/Measures/b13d64e0-b0fc-42ad-bcb1-38ee17063d2b.pdf>
- Camargo, L. (2017). El efecto Bitcoin en la economía colombiana, Colombia, Bogotá, recuperado de: <https://repository.unimilitar.edu.co/bitstream/handle/10654/16912/CamargoRicoLuzYenly2017.pdf;sequence=1>
- Caro y Obando. (2017). Monedas virtuales como una nueva alternativa de inversión, y su tendencia a través del tiempo, Medellín.
- Coinmarketcap. (2018), recuperado de: <http://coinmarketcap.com/all/views/all/>
- Castellanos, E. (2017) Criptomonedas, Blockchain y una nueva visión del mundo, Colombia, Medellín, recuperado de: <http://codeamed.com.co/wp-content/uploads/2018/05/Erick-Castellanos-Criptomonedas-Blockchain-y-una-nueva-visi%C3%B3n-del-mundo.pdf>

Castro, S. (2017). Blockchain, mirando más allá del Bitcoin, Colombia, Bogotá, recuperado de: [https://miethereum.com/wp-content/uploads/2017/11/Blockchain - mirando-mas-alla-de- Bitcoin.pdf](https://miethereum.com/wp-content/uploads/2017/11/Blockchain-mirando-mas-alla-de-Bitcoin.pdf)

CEF, Centro de Estudios Financieros. (2017). Bitcoin y Criptomonedas, Tema de análisis/#4, Trabajo de investigación, SESE, ESE. Business School, Universidad de los Andes, Bogotá Distrito Capital, Colombia, recuperado de: [https://www.ese.cl/ese/site/artic/20180514/asocfile/20180514111252/bitcoin\\_y\\_criptomonedas.pdf](https://www.ese.cl/ese/site/artic/20180514/asocfile/20180514111252/bitcoin_y_criptomonedas.pdf)

Coinmap. (2019). Mapa de establecimientos que manejan Bitcoin, recuperado de: <https://coinmap.org/#/map/5.14702454/-74.50378418/9>.

Condusef. (2019). Criptomonedas: cinco cosas que debes saber de ellas, Mexico, recuperado de: <https://www.condusef.gob.mx/>

CR Consultores Colombia. (2017). Concepto 8234, Monedas virtuales “Bitcoin” riesgos en su utilización, recuperado de: [http://crconsultorescolombia.com/concepto-8234 -monedas-virtuales-bitcoin-riesgos-utilizacion.php](http://crconsultorescolombia.com/concepto-8234-monedas-virtuales-bitcoin-riesgos-utilizacion.php)

Domínguez, J.; Lúquez, W. (2018) Implicaciones contables del Bitcoin y otras criptomonedas, España: Universidad de la Laguna, recuperado de: <https://riull.ull.es/xmlui/bitstream/handle/915/9251/Implicaciones%20contables%20del%20Bitcoin%20y%20otras%20criptomonedas..pdf?sequence=1&isAllowed=y>

Esparragoza, L. (2018). Cryptojacking obliga a universidad canadiense a apagar sus sistemas, Criptonoticias, recuperado de: <https://www.criptonoticias.com/seguridad/cryptojacking-obliga-universidad-canadiense-apagar-sistemas/>

Ethereum. (2018). Etéreo, recuperado de: <https://www.ethereum.org/>.

Fondo Monetario Internacional, (2018). Finanzas y desarrollo, Qué son las criptomonedas, Investigación financiera, recuperado de: <https://www.imf.org/external/pubs/ft/fandd/spa/2018/06/index.htm>

Herrera, J. (2016). Análisis y comparación de monedas criptográficas basadas en la tecnología Blockchain, España, Barcelona.

Gaitán, G. (2018) Criptomonedas o monedas virtuales, Colombia, Bogotá, recuperado de: <http://www.ctcp.gov.co/CMSPages/GetFile.aspx?guid=a201b2c9-5807-45b0-aeb6-35cacd43a864>

Guzmán, D. y Mesa, C., (2014). Bitcoin en Colombia, Colombia, Pereira, recuperado de: [http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/5153/33249G993 .pdf?sequence=1](http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/5153/33249G993.pdf?sequence=1)

Iglesias, A. (2016). Bitcoin y el cambio de divisa, España: Universidad Pontificia Comillas ICAI-ICADE.

López, E. (2017). El bitcoin supera los 11.000 dólares y dobla su cotización desde octubre, España, Barcelona, recuperado de: <https://www.elperiodico.com/es/economia/20171128/el-bitcoin-roza-los-10000-dolares-y-dobla-su-cotizacion-desde-octubre-6454190>.

López, B. (2018) Estudio de tecnologías Bitcoin y Blockchain, España, Cataluña, recuperado de: [http://openaccess.uoc.edu/webapps/o2/bitstream/10609/81739/7/blopezroTFM0618 memoria.pdf](http://openaccess.uoc.edu/webapps/o2/bitstream/10609/81739/7/blopezroTFM0618%20memoria.pdf)

Martinez, J. (2014). Bitcoins. ¿Revolución o historia?, España, Madrid, recuperado de: <https://repositorio.comillas.edu/jspui/bitstream/11531/70/1/TFG000011.pdf>

Ordinas, M. (2017). Las criptomonedas: ¿oportunidad o burbuja? España: Banca March.

Pallares, R. (2014). ¿Son las monedas virtuales el futuro de las finanzas internacionales? Investigación académica, Argentina.

Pérez, D. (2018) Bitcoin Gold sufre un ataque de doble gasto: Los exchanges pierden millones. Recuperado de: <https://tecnonucleous.com/2018/05/24/bitcoin-gold-sufre-un-ataque-de-doble-gasto/>

Ripple. (2018). Join RippleNet, recuperado de: <https://ripple.com/>.

Rivas, P. (2016). La inclusión del Bitcoin en el marco de la soberanía monetaria y la supervisión por riesgos en Colombia, Colombia: Universidad de los Andes.

Rodriguez, M. (2014). La tecnología Blockchain y su aplicabilidad en la contabilidad. De la partida doble al sistema de triple entrada, España, La Coruña, recuperado de: <https://aece.es/wp-content/uploads/2014/05/70g.pdf>.

Salinas, M. (2017). Bitcoin: una visión general, México, recuperado de: <http://www.revista.unam.mx/vol.18/num1/art11/art11.pdf>

Sarmiento, J. y Garcés, J. (2016). Criptodivisas en el entorno global y su incidencia en Colombia, Colombia: Universidad Santo Tomás, Santa fe de Bogotá.

SCProgress. (2017). Criptomonedas, Ecuador, recuperado de: <https://www.scprogress.com/NOTICIAS/e-commerce7-20170710.pdf>

Superintendencia Financiera de Colombia. (2014). Monedas Virtuales, Colombia, Bogotá, recuperado de: <https://www.superfinanciera.gov.co/inicio/10082781>.

Tenorio, K. (2018). Criptomonedas, México, recuperado de: <file:///C:/Users/Felipe%20Perdomo/Downloads/CESOP-IL-72-14-Criptomonedas-130418.pdf>.

Universidad de los Andes. (2018) ¿Tienen las criptomonedas los atributos necesarios para reemplazar al dinero actual? Posición del banco de pagos internacionales (bis) - reporte económico anual - junio 2018, Colombia, Bogotá, recuperado de: [https://ese.cl/ese/site/artic/20181029/asocfile/20181029134139/documento\\_n\\_\\_15\\_\\_agosto\\_2018.pdf](https://ese.cl/ese/site/artic/20181029/asocfile/20181029134139/documento_n__15__agosto_2018.pdf)

University of Birmingham (2017) Digital Cash, Reino Unido, Birmingham.

Viales, R. (2008). La evolución histórica de la moneda y de los sistemas monetarios. Bases conceptuales para estudiar la historia monetaria, Universidad de Costa Rica, San Pedro de Montes, Costa Rica, recuperado de: <https://www.redalyc.org/pdf/439/43913132011.pdf>

## ANEXOS

### ANEXO 1. Formato de entrevista abierta semiestructurada

#### PROPUESTA DE ENTREVISTA

A: YO

B: PERSONA ENTREVISTADA

A: Buenos días Sr. Hernando Fernández, gracias por recibirme y dedicarme un poco de su valioso tiempo.

B:

A: Primero que todo, cuéntenos un poco de su nivel de escolaridad.

B:

A: Puede comentarme acerca de sus actividades diarias en este mercado.

B:

A. Quisiera saber de su experiencia en el mercado.

B:

A: Su experiencia es excelente y gratificante, cuenta con un perfil propicio para hablar del tema de las criptomonedas. Puede realizar una pequeña introducción de este mercado de las criptomonedas.

B:

A: Comente acerca de la criptomoneda más importante

B:

A: ¿Considera que las criptomonedas son el boom de este siglo? ¿Por qué?

B:

A: Sin duda alguna todo lo que usted nos cuenta es importante, quisiera adentrar un poco al tema del doble gasto, ¿ha escuchado acerca de esto?

B:

A. Puede plantear un ejemplo de este problema.

B:

A: ¿Desde cuándo conoce este doble gasto?

B:

A: ¿Cuál es el proceso del doble gasto en Colombia?

B:

A: ¿Conoce casos de doble gasto en Colombia?

B:

A: ¿Conoce usted el reflejo de este problema en la contabilidad?

B:

A: ¿El Blockchain soluciona realmente este problema?

B:

A: ¿Se hace necesario una regulación acerca del tema de las criptomonedas en Colombia?

B:

A: ¿Cuáles podrían ser los efectos enfocados al doble gasto de esta regulación en las criptomonedas?

B:

A: Muchas gracias por esta amena conversación.

A: ESTUDIANTE

B: HERNANDO FERNÁNDEZ

A: Buenos días Sr. Hernando Fernández, gracias por recibirme y dedicarme un poco de su valioso tiempo.

B: Buenos días, con gusto, emocionado de poder seguir compartiendo información acerca de esta tecnología, para mi es una pasión que las personas entiendan el impacto disruptivo que esta tecnología está ocasionando, porque ya no es el futuro, está sucediendo.

A: Primero que todo, cuéntenos un poco de su nivel de escolaridad.

B: Nací en Colombia, viví hasta los 18 años, inicié dos carreras, contabilidad y finanzas e ingeniería industrial pero ninguna las terminé, llegue a los Estados Unidos en el año 2004 y empecé a cuestionar muchas cosas del sistema educativo y fue una decisión mía quedarme que no compartió mi familia, no continúe la universidad e inicié trabajando en múltiples trabajos, después de año y medio de estar en Estados Unidos el padre de un amigo me invita a trabajar en un call center de una empresa que hacía

hipotecas que ofrecía créditos hipotecarios, demore una semana en el call center y solicité que me pasaran como agente hipotecario, era una decisión bastante compleja porque no tenía ninguna remuneración pero me gustó tanto el tema e inicié, fueron 4 o 5 meses sin ganar dinero, fueron bastante duros hasta que por la pasión que le encontré y la vocación que le encontré a esa actividad me llené de información y esa fue mi mejor estrategia, inicio haciendo hipotecas y colapso cuando colapsó la economía en el año 2008, prácticamente lo perdí todo y me quedó una curiosidad muy grande de como el país más poderoso podía estar en banca rota y eso me llevó a investigar, me llevó a los libros y hacer muchas investigaciones en internet y empecé a encontrar un montón de respuestas acerca de cómo en realidad funciona el dinero y me obsesioné a estudiar la historia del dinero de realmente cómo llegamos a tener billetes, monedas, cómo funcionan las economías de los países, qué es el dólar, por qué el dólar es la moneda más importante a nivel global y fue un tema bastante fascinante, desde el 2008 al 2016 tuve la oportunidad de reestablecerme financieramente, continué en bienes raíces desde otro ángulo, dejé de hacer hipotecas y empecé a crear pequeños fondos de inversiones con amigos donde compraba bienes en remate y hasta el año 2016 una persona me presenta el White Paper de Satoshi Nakamoto, ese punto fue un antes y un después de como yo percibí el dinero como tal porque encontré una solución gigante a todas las dudas que se me crearon de las investigaciones de cómo funciona el dinero.

A: Puede comentarme acerca de sus actividades diarias en este mercado.

B. Sigo envuelto en bienes raíces y una de mis metas es poder combinar a nivel global la tecnología *Blockchain* con las inversiones inmobiliarias, si usamos Colombia como ejemplo para comprar una propiedad lleva un proceso y lo que valida que tú eres el propietario es la escritura que reposa en la notaría, si esa propiedad tiene 4 dueños y tú eres uno de los dueños y necesitas dinero y quieres usarla como colateral tienes que pedirle permiso a los otros 3 socios para que te aprueben la hipoteca, con *Blockchain* ese problema desaparece porque la propiedad como tal puede ser fraccionada y sigue siendo una propiedad, sigue siendo una escritura pero puede estar fraccionada en 4 y tú puedes pedir una hipoteca usando tu porcentaje que es el 25% como colateral sin que afecte a las otras 3 personas ni mucho menos tenga que pedirle permiso, eso cambia completamente la dinámica de como nosotros hacemos transacciones inmobiliarias a nivel global no solo en Colombia. Mi perfil en redes sociales está muy enfocado en la tecnología *Blockchain* porque me enamoré de ella, tengo mucho tiempo envuelto en ella y también participo en varios proyectos como asesor y consultor de empresas que quieren adoptar la tecnología y cualquier proyecto que tenga interés en ser lanzado al mercado si yo le veo futuro y pueda resolver un problema.

A. Quisiera saber de su experiencia en el mercado.

B: Ha sido una experiencia maravillosa, yo me motivé a desarrollar y enfocar mi perfil social en *Blockchain* y criptomonedas por un problema que detecté, en el año 2017 en múltiples países hubo una vitalización de pirámides, donde muchas personas fueron afectadas y perdieron su dinero por una sencilla razón y es desconocimiento y no encontrar fuentes de información que puedan tomar decisiones objetivas y empecé a educar y compartir no solo las definiciones de la tecnología y el impacto de las

criptomonedas sino mi opinión de esta tecnología como tal y eso fue lo que hizo que se viralizara mi perfil.

A: Su experiencia es excelente y gratificante, cuenta con un perfil propicio para hablar del tema de las criptomonedas. Puede realizar una pequeña introducción de este mercado de las criptomonedas.

B: No solo el mercado de las criptomonedas, hay algo que quisiera resaltar y que me parece extremadamente importante y es analizar un poco la historia detrás de la historia, si nos ponemos a pensar que sucedió cuando internet llegó al mundo, que hizo internet, nos ponemos analizar ese impacto tan fuerte que tuvo y voy a usar un ejemplo muy puntual cuando y tenía 15 años recuerdo que hacía las tareas usando la biblioteca de mi abuelo donde tomaba módulos de enciclopedias, esta industria era extremadamente poderosa porque la información estaba centralizada totalmente y una industria de 240 años cuando internet apareció la borró del mapa completamente porque la información cuando llega a internet se descentraliza, anteriormente tenía compañeros que no tenían acceso a la enciclopedia y tenían que apoyarse de mi persona para presentar sus tareas, internet cambió esa necesidad porque la información se descentralizó y lo mismo que hizo internet a las enciclopedias se lo va hacer *Blockchain* a muchísimas industrias, aquí al final se define todo en la credibilidad, todo está apalancado en la credibilidad, si revisamos *Wikipedia* es una plataforma que es actualizada a diario, no tiene un ente central pero es una de las fuentes más creíbles porque es casi imposible que tantas personas estén equivocadas, entonces es un consenso de información que se actualiza diariamente, dicho esto las criptomonedas no son más que el primer uso o representación de la tecnología *Blockchain* especialmente *Bitcoin*.

Las criptomonedas las podemos ver como medio de pago o como registros inmutables, hoy en día en Colombia para comprar un vehículo tiene que estar registrado con una tarjeta de propiedad, ese departamento donde se registra es centralizado y es controlado por el gobierno, con *Blochckain* no es necesario que un ente tenga el control y que este centralizado, si es necesario que un ente lo regule pero los gobiernos y servidores son vulnerables a que hayan errores tanto humanos o malintencionados. *Bitcoin* tuvo la intención de ser un medio de pago pero en mi concepto personal *Bitcoin* no va ser un medio de pago, *Bitcoin* va ser el reemplazo del oro, yo lo llamo Oro 2.0, porque si vamos a la historia del dinero nos damos cuenta que este metal precioso tiene todos los elementos necesarios para ser una reserva de riqueza, el papel moneda como tal no.

A: Puede comentar acerca de la criptomoneda más importante

B: Primero la preocupación mayor que tienen las personas es acerca del Pseudónimo Satoshi Nakamoto, pero no importa quién lo haya desarrollado se puede depositar la confianza en la tecnología como tal porque funciona, *Bitcoin* nace como una rebelión de lo que sucedió en el año 2008 en Estados Unidos donde el sistema bancario para resolver la crisis que hubo como tal lo que hicieron fue imprimir más dinero básicamente, entonces en el 2008 se crea el White Paper con la intención de que a largo plazo *Bitcoin* se convirtiera como la criptomoneda que reemplazaría el papel moneda y el medio de pago más importante y creíble del mundo, en mi concepto personal no va ser un medio de pago va ser oro 2.0 como te lo dije por la fluctuación que tiene esta criptomoneda, tú no

puedes tener la tranquilidad de que si vendes tu casa o carro recibir un pago hoy y que en 10 días hayas perdido un 10%, por eso *Bitcoin* no va ser un medio de pago, *Bitcoin* va ser una reserva de riqueza, así como el dólar estaba respaldado por oro hasta 1971, este es el nuevo oro, cual es la ventaja, que no tiene que guardarlo en bodegas, no tienes que gastar en altos niveles de seguridad, transportarlos no es un problema, entonces cuando empezamos a comparar las características de que tiene *Bitcoin* mejor sobre el oro, es que es realmente finito, no se pueden crear más de 21 millones de monedas que son las que tiene el algoritmo establecido, realmente no se sabe cuánto oro hay en el mundo, hay una estimación pero nadie tiene exactitud de cuanto oro hay en el mundo.

A: ¿Considera que las criptomonedas son el boom de este siglo? ¿Por qué?

B: Yo considero que es la tecnología que más impacto va tener después de internet, *Blockchain* y *Bitcoin* como tal va a ser una nueva fuente de guardar riqueza que cada día las personas se están educando y entendiendo realmente que es esto, el mayor problema que sucedió en Colombia es que la mayoría de personas que conocieron *Bitcoin* lo quisieron usar como un método para enriquecerse y no es un método para esto, tu no compras dólares para enriquecerte, tu compras dólares porque vas viajar y los necesitas o porque piensas que eso puede guardar más el valor que el peso colombiano, cuando las personas tienen una percepción y le dan un uso diferente al que realmente es, sucede todo lo que ha sucedido no solo en Colombia sino en Latinoamérica, yo recibía aproximadamente 120 mensajes diarios en el año 2017 exactamente en diciembre, cuando las personas empezaron a notar que en ese año en enero empezó en 800 dólares promedio y en diciembre llegó a casi 20.000 dólares, eso fue un incremento desproporcional.

A: Sin duda alguna todo lo que usted nos cuenta es importante, quisiera adentrar un poco al tema del doble gasto, ¿ha escuchado acerca de esto?

B: Si claro y lo conozco perfectamente, en el tema de economía lo manejo bastante bien y de hecho a una profundidad interesante, el tema del doble gasto es un problema que el efectivo no tiene, si tú pagas una hamburguesa con 10.000 pesos cuando el mesero te traiga la cuenta esos 10.000 pesos salieron de tu bolsillo y entraron al bolsillo del restaurante, ahí el efectivo no tiene ese problema, en una transacción digital si se puede presentar ese problema. Imagina que tienes un *Bitcoin* en tu billetera y tratas de gastarlo dos veces en dos transacciones diferentes, tratando de enviar el mismo *Bitcoin* a dos billeteras separadas, ambas de estas transacciones pasan al grupo de transacciones no confirmadas, entonces la primera transacción se aprobaría a través del mecanismo de confirmación que en *Bitcoin* son los mineros. Los mineros juegan un papel crucial en la solución del problema del doble gasto porque son notarios que están validando transacciones constantemente, como te decía la primera transacción la aprueban y queda registrada en un bloque, los bloques en *Bitcoin* se cierran cada 10 minutos, si comparamos en un banco o en un restaurante cierran caja dos veces al día o tres, la contabilidad de *Bitcoin* cierra caja cada 10 minutos, cada 10 minutos se cierra un bloque, entonces la primera transacción se valida y se confirma, la segunda sería reconocida como no valida o rechazada, sucedería algo muy similar a cuando pasas una tarjeta por un datafono y te dice fondos insuficientes, si ambas transacciones suceden simultáneamente

prevalecerá la que más confirmaciones tenga por parte de esos mineros, los mineros lo único que hacen es que validan que el registro contable esté en orden.

A: Puede plantear un ejemplo de este problema.

B: Cuando tú vas a pagar en cualquier lado y pasas la tarjeta, no voy a utilizar el efectivo porque no tiene este problema, cuando tú sacas un billete de tu bolsillo y lo entregas al establecimiento que le pagaste, ese dinero salió de tu bolsillo e ingreso a la caja del restaurante, pero cuando vamos a transacciones digitales cuando vamos a dinero digital este problema si es vulnerable, *Blockchain* soluciona que cuando tu pases tu tarjeta débito o crédito y se valide la transacción, lo que hace *Blockchain* es el equivalente a las validaciones que hace *Visa* o *Mastercard* de conectarse y a través de internet validar con tu bancos si tienes los fondos disponibles y regresa esa señal bastante rápida y valida la transacción y entonces te la aprueba o te la rechaza sino tienes el saldo como tal, pero esto tiene que hacerlo un ente centralizado que en este caso es *Visa* o *Mastercard* que son los que validan a través de tecnología y recursos humanos, con *Blockchain* no se necesitan recursos humanos ni un ente centralizado, la tecnología permite validar que cuando salga dinero de tu billetera ya no va estar ahí y si ingrese a la billetera del destinatario, validándose por estos minero que son los que reemplazan la función de *Visa* o *Mastercard*.

A: ¿Desde cuándo conoce este doble gasto?

B: El doble gasto lo vi en la universidad y volvió aparecer cuando empecé a investigar la historia acerca del dinero, ahí fue donde profundicé y entendí que hasta que no apareciera una solución al doble gasto no iba a poderse evitar crisis como la que sucedió en el 2008.

El doble gasto aparece cuando empiezan hacerse transacciones digitales, desde que aparece una tarjeta de crédito o usas un plástico hay una vulnerabilidad del doble gasto, desde que se utilizan las tarjetas se puede hablar de doble gasto, eso puede ser un referente.

A: ¿Cuál es el proceso del doble gasto en Colombia?

B: No importa donde ocurra el doble gasto, sigue siendo un problema porque es un problema de dinero digital o de pagos digitales, en lo físico no existe doble gasto pero si lo miramos desde el punto de vista digital tenía que existir anteriormente un ente que evitara el doble gasto, la tecnología *Blockchain* no necesita un ente, esta se encarga de que esto no suceda.

A: ¿Conoce casos de doble gasto en Colombia?

B: No, casos puntuales de doble gasto que hayan sucedido no tengo conocimiento.

A: ¿Conoce usted el reflejo de este problema en la contabilidad?

B: No tanto como se refleja sino lo que si tengo claro es el impacto que altera completamente la contabilidad, desbalancea cualquier registro contable y cualquier sistema contable que tenga un problema de doble gasto pierde la credibilidad de los

usuarios de inmediato. Nosotros como seres humanos desconfiamos unos de otros y por eso recurrimos a un tercero para que nos regule.

A: ¿El *Blockchain* soluciona realmente este problema?

B: 100%

A: ¿Se hace necesario una regulación acerca del tema de las criptomonedas en Colombia?

B: Lógicamente es necesaria la regulación pero desde mi punto de vista los gobiernos tienen que hacer una regulación con una adopción de la tecnología, *Blockchain* no lo van a regular los gobiernos, no lo pueden manipular los gobiernos, es *Blockchain* quien termina creando nuevas reglas a las cuales los gobiernos tienen que adaptarse.

A: ¿Cuáles podrían ser los efectos enfocados al doble gasto de esta regulación en las criptomonedas?

B: Que sucede si el gobierno colombiano no adopta las criptomonedas en mi criterio personal va ocurrir primero la evasión más grande de impuestos de la historia y segundo el lavado de dinero se va incrementar exponencialmente, esas son las dos consecuencias desde el punto de vista financiero si miramos el *Bitcoin* como medio de pago porque en Colombia hay demasiada exclusión y falta de inclusión de todos los colombianos en el sistema bancario, la informalidad en Colombia es el día a día. Si te haces la pregunta, cuantas personas en Colombia no tienen una cuenta de banco, cuantas pueden y no quieren, debido a que por guardar el dinero te cobran una cuota mensual, si sacas dinero y lo metes varias veces el 4xmil te acaba, entonces las personas de la nueva generación poco a poco se han dado cuenta que no necesitan utilizar este sistema y empiezan a utilizar este otro sistema, así como nuestros padres y abuelos solamente podían buscar información en las enciclopedias, hoy en día los milenials no tienen ese inconveniente porque entienden que en el internet la pueden encontrar de manera práctica, simultáneamente puede suceder eso en el sistema financiero en Colombia entonces es extremadamente importante que haya una adopción y una regulación para que muchas más personas puedan utilizar esta tecnología pero sobretodo como lo hace el gobierno Americano y el gobierno Canadiense y todos los gobiernos de países desarrollados que saben que no pueden controlar esto pero por lo menos pueden tener una idea de lo que está sucediendo, pueden aplicar impuestos y pueden regular un poco este mundo que en estos momentos es completamente gris en Colombia. En el proyecto de ley que hay en el congreso no quieren que lo regule la Superfinanciera sino que están impulsando y promoviendo para que la Supersociedades sea quien lo regule como un activo y no como dinero. Hay un miedo gigante en donde piensan que se va a desbalancear el sistema financiero pero van a ser peor las consecuencias sino adoptan esta tecnología desde ya porque están estimulando la informalidad.

A: Muchas gracias por esta amena conversación.

## ANEXO 2. Formato recopilación de datos

DATOS GENERALES		
NOMBRE DOCUMENTO		
FECHA DEL DOCUMENTO		
FECHA DE CONSULTA		
LINK		
LUGAR		
DATOS		
<i>BITCOIN</i>	DOBLE GASTO	<i>BLOCKCHAIN</i>

MODELO DE AUTORÍA PROPIA

DATOS GENERALES		
<p>La criptomoneda <i>Bitcoin</i> opera sobre la tecnología de código abierto denominada blockchain. Este sistema se trata de una base de datos distribuida en ordenadores mediante red P2P, y en la que se almacenan en bloques todas las transacciones por orden cronológico que conforman una cadena de operación contable entre pares.</p>		
NOMBRE DOCUMENTO	Estudio de tecnologías <i>Bitcoin</i> y <i>Blockchain</i> .	
FECHA DEL DOCUMENTO		
FECHA DE CONSULTA	Abril 22 de 2019	
LINK	<a href="http://openaccess.uoc.edu/webapps/o2/bitstream/10609/81739/7/blopezroTFM0618memoria.pdf">http://openaccess.uoc.edu/webapps/o2/bitstream/10609/81739/7/blopezroTFM0618memoria.pdf</a>	
LUGAR	Cataluña, España	
DATOS		
<i>BITCOIN</i>	DOBLE GASTO	<i>BLOCKCHAIN</i>
<p>Características de <i>Bitcoin</i>:</p> <ul style="list-style-type: none"> <li>● Origen anónimo.</li> <li>● Código abierto.</li> <li>● Funciona sobre <i>Blockchain</i>.</li> <li>● Descentralizada.</li> <li>● No legislada.</li> </ul>	<p>El protocolo <i>Bitcoin</i> sobre la arquitectura P2P resuelve el problema de doble gasto que existía en intercambio de digital de dinero sin confirmación, y por el cual un comprado actuando de mala fe, podría realizar dos compras simultáneas usando el mismo dinero.</p>	<p><i>Blockchain</i> es un libro de contabilidad formado por registros (bloques) enlazados y cifrados para poder proteger la privacidad y seguridad de su actividad.</p> <p>Se eliminan intermediarios, pero las transacciones deben ser validadas igualmente.</p>

MODELO DE AUTORÍA PROPIA

DATOS GENERALES		
<p>La innovación tecnológica es el principal valor que ofrece <i>Bitcoin</i>, siendo la primera divisa digital que soluciona el problema del doble gasto para las transacciones a través de internet, sin recurrir a un tercer agente confiable.</p>		
NOMBRE DOCUMENTO	<i>Bitcoins. ¿Revolución o historia?</i>	
FECHA DEL DOCUMENTO	Junio de 2014	
FECHA DE CONSULTA	Mayo 05 de 2019	
LINK	<a href="https://repositorio.comillas.edu/jspui/bitstream/11531/70/1/TFG000011.pdf">https://repositorio.comillas.edu/jspui/bitstream/11531/70/1/TFG000011.pdf</a>	
LUGAR	Madrid, España	
DATOS		
<i>BITCOIN</i>	DOBLE GASTO	<i>BLOCKCHAIN</i>
<p><i>Bitcoin</i> es una moneda digital criptográfica que usa tecnología P2P para operar sin necesidad de una autoridad central o bancos, creada por Satoshi Nakamoto en 2009. <i>Bitcoin</i> es de código abierto lo que significa que su diseño es público y todo el mundo puede ver el código fuente que sustenta la red.</p>	<p>En una extracción monetaria de un banco o cajero, lo que ocurre es que antes de la retirada de efectivo el banco se encarga de comprobar el estado de la cuenta para la disposición de fondos. Una vez retirada la cantidad de dinero acorde al saldo de la cuenta, de nuevo el banco se encarga de ajustar el balance para que no ocurra un doble gasto, es decir, que no se utilice el mismo dinero dos veces.</p>	<p>No se encontraron datos del sistema <i>Blockchain</i>.</p>

MODELO DE AUTORÍA PROPIA

DATOS GENERALES		
<p>Las iniciativas de estas prestigiosas instituciones confirman que debemos dar a las criptomonedas y a <i>Blockchain</i> el papel protagónico que merecen. En efecto, generan una transformación radical del mundo que conocemos, que se fundamenta en registros centralizados e intermediarios, planteando un enorme reto a estos últimos, exigiéndoles que se apropien de esta transformación y se adapten a ella.</p>		
NOMBRE DOCUMENTO	Criptomonedas, <i>Blockchain</i> y una nueva visión del mundo.	
FECHA DEL DOCUMENTO	Octubre 26 de 2017	
FECHA DE CONSULTA	Mayo 15 de 2017	
LINK	<a href="http://codeamed.com.co/wp-content/uploads/2018/05/Erick-Castellanos-Criptomonedas-Blockchain-y-una-nueva-visi%C3%B3n-del-mundo.pdf">http://codeamed.com.co/wp-content/uploads/2018/05/Erick-Castellanos-Criptomonedas-Blockchain-y-una-nueva-visi%C3%B3n-del-mundo.pdf</a>	
LUGAR	Medellín, Colombia	
DATOS		
<i>BITCOIN</i>	DOBLE GASTO	<i>BLOCKCHAIN</i>
<p><i>Bitcoin</i> soluciona este inconveniente de los pagos directos, al ser una “versión totalmente peer-to-peer de dinero electrónico que permite que una parte haga pagos en línea a otra de manera directa, sin tener que acudir a una institución financiera.</p>	<p>El problema del doble gasto, el cual consiste en el riesgo de que se disponga de una unidad de moneda digital en dos lugares, de tal forma que uno de los pagos sea rechazado.</p>	<p>(Registro distribuido de transacciones que permite el funcionamiento de las criptomonedas).</p>

MODELO DE AUTORÍA PROPIA

DATOS GENERALES		
<p>Esta investigación pretende abordar la dinámica económica que ha introducido la nueva tecnología en la utilización del <i>Bitcoin</i> como criptomoneda para efectuar transacciones de pago y transferencias de dinero digital sin control de las entidades financieras ni pago de impuestos.</p>		
NOMBRE DOCUMENTO	El efecto <i>Bitcoin</i> en la economía colombiana.	
FECHA DEL DOCUMENTO	2017	
FECHA DE CONSULTA	Mayo 7 de 2019	
LINK	<a href="https://repository.unimilitar.edu.co/bitstream/handle/10654/16912/CamargoRicoLuzYenly2017.pdf;jsessionid=6BE9D072F41C2C03A40D81D91136B0C2?sequence=1">https://repository.unimilitar.edu.co/bitstream/handle/10654/16912/CamargoRicoLuzYenly2017.pdf;jsessionid=6BE9D072F41C2C03A40D81D91136B0C2?sequence=1</a>	
LUGAR	Bogotá, Colombia	
DATOS		
<i>BITCOIN</i>	DOBLE GASTO	<i>BLOCKCHAIN</i>
<p><i>Bitcoin</i> es la primera moneda descentralizada que utiliza el internet para enviar dinero directamente de persona a persona a cualquier parte del mundo las 24 horas sin tener que utilizar una entidad centralizada, un banco, PayPal o western unión</p>	<p>Posibilidad de que los <i>Bitcoins</i> sean gastados más de una vez por la misma persona.</p>	<p>Al resolver el problema se verifica la exactitud de la cadena de bloque o libro mayor de contabilidad <i>Blockchain</i>, el cual es público y en el que quedan registradas todas y cada una de las transacciones.</p> <p>Utiliza la cadena de bloques llamada "<i>Blockchain</i>" para registrar todas las transacciones e impedir el doble gasto.</p>

MODELO DE AUTORÍA PROPIA

DATOS GENERALES		
Este documento describe los esquemas de CA así como su tecnología subyacente, y presenta los beneficios, costos, riesgos y oportunidades asociados con dichos esquemas. De esta manera, se identifican los principales retos de política pública en esta materia.		
NOMBRE DOCUMENTO	Criptoactivos	
FECHA DEL DOCUMENTO		
FECHA DE CONSULTA	10 de mayo de 2019	
LINK	<a href="http://www.banrep.gov.co/docum/Lectura_finanzas/pdf/documento-tecnico-criptomonedas.pdf">http://www.banrep.gov.co/docum/Lectura_finanzas/pdf/documento-tecnico-criptomonedas.pdf</a>	
LUGAR	Colombia	
DATOS		
<i>BITCOIN</i>	DOBLE GASTO	<i>BLOCKCHAIN</i>
Conceptualmente, los CA como el <i>Bitcoin</i> son un caso particular de lo que se conoce como monedas virtuales. Estas se definen como unidades digitales susceptibles de ser usadas como medio de pago en el intercambio de bienes y servicios, como depósito de valor y como unidad de cuenta. Usualmente están denominadas en su propia unidad de cuenta y son guardadas, negociadas y transferidas electrónicamente (FATF, 2015).	El CA no pueda ser falsificado o utilizado por el mismo tenedor más de una vez ( <i>the double spending problem</i> , o el problema del gasto repetido o doble gasto); de tal manera que se preserve su valor adquisitivo. Así mismo, deben garantizar que su autenticidad sea fácilmente verificable al momento de hacer una transacción.	Estos esquemas utilizan la tecnología denominada de registro distribuido encriptado (DLT) o <i>Blockchain</i> , para llevar la historia transaccional completa del activo digital entre cuentas de distintos participantes sin la necesidad de que sea intermediada por una contraparte centralizada.

MODELO DE AUTORÍA PROPIA

DATOS GENERALES		
<p>La tecnología subyacente a las criptomonedas denominada <i>Blockchain</i> o cadena de bloques podría ser prometedora en otras aplicaciones, como la simplificación de los procesos administrativos en la liquidación de actas, procesos de auditoría, registros contables o elaboración de contratos inteligentes. Por esto, es importante regular los usos públicos y privados de esta tecnología, discutir las medidas necesarias para prevenir el fraude y evaluar la posible emisión de monedas digitales por parte de los bancos centrales.</p>		
NOMBRE DOCUMENTO	¿Tienen las criptomonedas los atributos necesarios para reemplazar al dinero actual? Posición del banco de pagos internacionales (bis) - reporte económico anual - junio 2018	
FECHA DEL DOCUMENTO	Agosto 2018	
FECHA DE CONSULTA	Mayo 20 de 2019	
LINK	<a href="https://ese.cl/ese/site/artic/20181029/asocfile/20181029134139/documento_n__15__agosto_2018.pdf">https://ese.cl/ese/site/artic/20181029/asocfile/20181029134139/documento_n__15__agosto_2018.pdf</a>	
LUGAR	Bogotá, Colombia	
DATOS		
<i>BITCOIN</i>	DOBLE GASTO	<i>BLOCKCHAIN</i>
<p>El segundo tipo de criptomonedas se componen por una desviación mucho más radical de la configuración predominante basada en instituciones. Éstas prometen generar confianza en un entorno completamente descentralizado.</p>	<p>El desafío tecnológico en el intercambio digital entre pares (peer-to-peer) es el denominado "problema de doble gasto": cualquier forma de dinero digital es fácilmente replicable y, por lo tanto, se puede gastar fraudulentamente más de una vez, de hecho, es más fácil reproducir información digital que falsificar billetes bancarios.</p>	<p>El libro de contabilidad distribuido denominado <i>Blockchain</i> o cadena de bloques. Éste se actualiza en grupos de transacciones llamadas bloques.</p>

MODELO DE AUTORÍA PROPIA

DATOS GENERALES		
<p>Durante los últimos años, el término <i>Blockchain</i> ha ganado popularidad como una de las nuevas tecnologías con mayor poder para transformar la forma en que el sistema financiero ofrece productos y servicios a través de mejoras tanto en procesos operativos (<i>back-office</i>) como en interfaces y nuevas formas de interacción con el cliente (<i>frontoffice</i>).</p>		
NOMBRE DOCUMENTO	<i>Blockchain: mirando más allá del Bitcoin</i>	
FECHA DEL DOCUMENTO	Abril 03 de 2017	
FECHA DE CONSULTA	Mayo 15 de 2019	
LINK	<a href="https://miethereum.com/wp-content/uploads/2017/11/Blockchain-mirando-mas-alla-de-Bitcoin.pdf">https://miethereum.com/wp-content/uploads/2017/11/Blockchain-mirando-mas-alla-de-Bitcoin.pdf</a>	
LUGAR	Colombia	
DATOS		
<i>BITCOIN</i>	DOBLE GASTO	<i>BLOCKCHAIN</i>
<p>Bajo el seudónimo de Satoshi Nakamoto, el o los autores mostraron al mundo una versión de dinero electrónico cuyo fin era permitir la realización de pagos directos entre personas (<i>peerto-peer</i> o P2P) sin la necesidad de una institución financiera. Esto significó en términos más prácticos la creación de una nueva moneda, el <i>Bitcoin</i>.</p>	<p>El problema de doble gasto es una falla de los esquemas de dinero digital que consiste en que un solo token digital puede ser gastado dos veces. A diferencia del dinero físico como billetes y monedas, los archivos electrónicos pueden duplicarse y no evidenciar un cambio de titularidad (dueño) cuando es usado.</p>	<p>El <i>Blockchain</i> o cadena de bloques es un registro público de transacciones que se mantiene mediante una red distribuida de computadores, que no requiere respaldo de ninguna autoridad central o una tercera parte y que ofrece un esquema transaccional libre de intermediarios, gracias al uso de algoritmos criptográficos.</p>

MODELO DE AUTORÍA PROPIA

DATOS GENERALES		
El CTCP analiza las posibles categorías de activos en las que podrían ser clasificadas las criptomonedas, después de una consulta interpuesta por la codirectora del Banco de la República.		
NOMBRE DOCUMENTO	Criptomonedas o monedas virtuales	
FECHA DEL DOCUMENTO	Mayo 28 de 2018	
FECHA DE CONSULTA	Mayo 20 de 2019	
LINK	<a href="http://www.ctcp.gov.co/CMSPages/GetFile.aspx?guid=a201b2c9-5807-45b0-aeb6-35cacd43a864">http://www.ctcp.gov.co/CMSPages/GetFile.aspx?guid=a201b2c9-5807-45b0-aeb6-35cacd43a864</a>	
LUGAR	Bogotá, Colombia	
DATOS		
<i>BITCOIN</i>	DOBLE GASTO	<i>BLOCKCHAIN</i>
No se encontraron datos del <i>Bitcoin</i> .	No se encontraron datos del doble gasto.	No se encontraron datos del sistema <i>Blockchain</i> .

MODELO DE AUTORÍA PROPIA

DATOS GENERALES		
<p>Este trabajo pretende aportar un panorama del sistema de pago <i>Bitcoin</i> describiendo su funcionamiento, arquitectura, modo de operación y algunas de las consideraciones financieras asociadas; se espera que este escrito pueda ser utilizado como una introducción para quien se encuentre interesado en el estudio del tema.</p>		
NOMBRE DOCUMENTO	<i>Bitcoin: una visión general</i>	
FECHA DEL DOCUMENTO	Enero 1 de 2017	
FECHA DE CONSULTA	Mayo 20 de 2019	
LINK	<a href="http://www.revista.unam.mx/vol.18/num1/art11/art11.pdf">http://www.revista.unam.mx/vol.18/num1/art11/art11.pdf</a>	
LUGAR	Ciudad de México, México	
DATOS		
<i>BITCOIN</i>	DOBLE GASTO	<i>BLOCKCHAIN</i>
<p><i>Bitcoin</i> es un sistema de pago electrónico que desde su aparición en 2009 se ha posicionado como uno de los de mayor uso, dando pie a que diversas empresas alrededor del mundo lo promuevan y adopten.</p>	<p>El trabajo de los mineros comienza con la labor de agrupar las transacciones en un bloque para verificar su validez, es decir, comprobar la procedencia de las monedas para garantizar que no son falsificadas o que no hayan sido gastadas con anterioridad (prevenir el doble gasto).</p>	<p>Es el registro histórico de las transacciones que se han llevado a cabo en el sistema. Se organiza mediante bloques, que son conjuntos de direcciones.</p>

MODELO DE AUTORÍA PROPIA

## ANEXO 3. Foto entrevista aplicada a experto en el tema

