

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 4221 de 7 de junio de 2019

Ref. Expediente N° NC2018/0011415

Señor(a)
BLACK GOLD COIN INC.

TÍTULO DE LA SOLICITUD: **“SISTEMAS Y MÉTODOS PARA PROPORCIONAR UNA VERIFICACIÓN DE IDENTIDAD PERSONAL MULTIFACTORIAL BASADA EN UNA CADENA DE BLOQUES”**

NÚMERO DE SOLICITUD INTERNACIONAL: PCT/US2016/024776

FECHA DE PRESENTACIÓN INTERNACIONAL: 29 de marzo de 2016.

PRIORIDAD(ES): 28/03/2016, US (ESTADOS UNIDOS DE AMÉRICA), 15/083,241

Como resultado del examen de patentabilidad realizado a la solicitud indicada en la referencia, atendiendo a lo consagrado en el artículo 45 de la Decisión 486 de 2000, se le comunica que esta Dirección ha encontrado que la materia objeto de solicitud no cumple con algunos requisitos establecidos en la Decisión, con fundamento en los siguientes aspectos:

1. Modificaciones presentadas (Art. 34 Decisión 486)

La modificación de las reivindicaciones 1 a 20, radicadas mediante escrito N° NC2018/0011672, del 29 de octubre de 2018, no es aceptable porque la materia relacionada con “(...) donde cada uno de los siguientes: el identificador, el primer hash biométrico, el segundo hash biométrico, la primera dirección de verificación y la segunda dirección de verificación son diferentes entre sí, son diferentes de las primeras claves privadas y públicas de las cuales se derivó la primera dirección de verificación, y son diferentes de las segundas claves privadas y públicas de las cuales se derivó la segunda dirección de verificación;

obtenga, desde un dispositivo del lado del cliente, el identificador, los primeros datos biométricos, y los segundos datos biométricos en relación con una petición de verificación de la identidad del individuo, indicando la petición la primera dirección de verificación asociada con la cadena de bloques y la segunda dirección de verificación asociada con la cadena de bloques;

obtenga (i) el identificador almacenado y el primer hash biométrico almacenado utilizando la primera dirección de verificación indicada en la petición y (ii) el segundo hash biométrico almacenado utilizando la segunda dirección de verificación indicada en la petición; y firme, utilizando la clave privada de la cual se derivó la primera dirección de verificación, la verificación de la identidad del individuo como respuesta a una determinación en cuanto a que el identificador de la petición, los primeros datos biométricos de la petición, y los segundos datos biométricos de la petición coinciden con el identificador almacenado, el primer hash biométrico almacenado y el segundo hash biométrico almacenado;

proporciona a un primer usuario, que no es el individuo, acceso a los datos almacenados en uno o varios medios de almacenamiento legibles por una computadora en asociación con la primera dirección de verificación asociada con la cadena de bloques, donde se le proporciona acceso al primer usuario a los datos almacenados basándose en la verificación de que el primer usuario tiene una primera clave privada, siendo diferente la primera clave privada de la clave privada de la cual se derivó la primera dirección de verificación y siendo diferente de la clave privada de la cual se derivó la segunda dirección de verificación; y niegue a un segundo usuario, que no es el individuo, el acceso a los datos almacenados basándose en la verificación de que el segundo usuario tiene una segunda clave privada” (Reiv. 20) no había sido considerada inicialmente, por lo cual se amplía el objeto de la solicitud.

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 4221 de 7 de junio de 2019

Ref. Expediente N° NC2018/0011415

2. Objeto de la invención

De acuerdo con lo establecido en el numeral 1.2.2.2 del Capítulo Primero del Título X de la Circular Única para efectos del examen de patentabilidad, cuando la solicitud contenga más de diez (10) reivindicaciones y no se haya pagado la tasa complementaria, sólo se estudiarán las cubiertas por la tasa pagada al momento de realizar el examen de patentabilidad consagrado en el artículo 45 de la Decisión 486. Por lo tanto, se estudiarán las reivindicaciones 1 a 10 del radicado N° NC2018/0011415 del 25 de octubre de 2018.

El problema planteado en esta solicitud consiste en la necesidad de suministrar sistemas y métodos que proporcionen una verificación de la identidad de uno o varios individuos basada en una cadena de bloques, permitiendo que la verificación del usuario esté relacionada con los bloques anteriores encadenados al usuario, con el fin de aumentar la seguridad al acceso de la información del usuario.

Para resolver este problema técnico, la solicitud en estudio proporciona sistemas y métodos para proporcionar una verificación de identidad personal multifactorial basada en una cadena de bloques. Se puede incluir uno o más procesadores configurados mediante instrucciones legibles por una máquina para establecer direcciones de verificación en una cadena de bloques y/o llevar a cabo la verificación de identidad personal multifactorial basada en una cadena de bloques utilizando las direcciones de verificación. El establecimiento de las direcciones de verificación en la cadena de bloques puede incluir la asociación de identificadores con individuos habiendo verificado previamente las identidades personales, asociándose un primer identificador con un primer individuo, donde el primer individuo tiene una identidad personal previamente verificada; la asignación de direcciones de verificación en una cadena de bloques a los individuos, donde una dirección de verificación determinada incluye una clave pública y una clave privada, asignándose una primera dirección de verificación al primer individuo, donde la primera dirección de verificación incluye una primera clave pública y una primera clave privada.

3. De la solicitud de patente

3.1. Improcedencia del reconocimiento del resultado de examen de patentabilidad de solicitud extranjera (Art 46 D486)

La solicitud en trámite, que presentó el procedimiento acelerado de exámenes de patente (PPH) no puede ser concedida tal como fue concedida mediante la patente Estadounidense US 9,985,964, porque no cumple con los requisitos necesarios contemplados en Colombia de acuerdo a lo establecido en la Decisión 486, esto se debe a que la materia que fue otorgada por la oficina americana, amplía la materia presentada bajo la solicitud en estudio. Por el contrario, el solicitante presenta el capítulo reivindicatorio como fue concedido y que corresponde al pliego reivindicatorio modificado bajo el radicado N° NC2018/0011672 del 29 de octubre de 2018, del cual no fue aceptada la modificación del pliego reivindicatorio, toda vez que incluye características técnicas que no había sido divulgadas en la presentación inicial del presente trámite, como se evidencio en el numeral primera de la presente comunicación. Por lo tanto, es procedente realizar el requerimiento de 45.

3.2. Título

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 4221 de 7 de junio de 2019

Ref. Expediente N° NC2018/0011415

El nombre de la invención de que se trata en el artículo 27 literal d) de la Decisión 486 deberá reflejar el objeto y el campo industrial con el cual se relaciona la misma y ser concordante con la materia descrita y las reivindicaciones de la solicitud. El nombre no podrá referirse a nombres personales, marcas de productos o nombres de fantasía.

El solicitante en el escrito radicado bajo el N° NC2018/0011415 el 25 de octubre de 2018, tituló la invención como: “SISTEMAS Y MÉTODOS PARA PROPORCIONAR UNA VERIFICACIÓN DE IDENTIDAD PERSONAL MULTIFACTORIAL BASADA EN UNA CADENA DE BLOQUES”. Este título no se relaciona con el objeto de la solicitud contenido en la descripción y las reivindicaciones, por lo cual se sugiere el título siguiente: “SISTEMAS Y MÉTODOS PARA PROPORCIONAR UNA VERIFICACIÓN DE IDENTIDAD PERSONAL MULTIFACTORIAL BASADA EN UNA CADENA DE BLOQUES QUE PERMITE ASIGNAR UNA DIRECCIÓN DE VERIFICACIÓN EN RELACIÓN CON UN IDENTIFICADOR DE INDIVIDUO E INFORMACIÓN BIOMÉTRICA”.

3.3. Reivindicaciones (Art. 30 Decisión 486)

- Las reivindicaciones 1, 4 y 10 no son claras porque el término “*hardware*” es de carácter general que sugieren de forma imprecisa que la protección se extendería a posibles variaciones o modificaciones. Se sugiere sustituirlo por un término preciso.
- Se sugiere incluir entre paréntesis () los números de referencia de cada uno de los elementos que hacen parte de la invención de acuerdo con la numeración empleada en los dibujos, con el fin, de hacer más fácil la comprensión de la materia reivindicada.

4. Determinación del Estado de la Técnica

La fecha para determinar el estado de la técnica es el 28 de marzo de 2016 que corresponde a la fecha de presentación de la solicitud de prioridad.

Consultadas las fuentes de información con que se cuenta, se encontraron los siguientes documentos que anticipan el objeto de esta solicitud:

Ítem	Documento	Título	Fecha de Publicación
D1	US20150324789	“Cryptocurrency Virtual Wallet System and Method”	12 de noviembre de 2015
D2	US20150356555	“System and method for executing financial transactions”	10 de diciembre de 2015

El documento D1¹ divulga un método en el que se recibe una solicitud cifrada para transferir una cantidad solicitada de criptomoneda desde una dirección de usuario a una dirección de destino. La solicitud incluye una dirección de destino, una cantidad solicitada, una clave de cifrado del dispositivo del usuario y datos biométricos. También se recibe una transacción parcialmente firmada para transferir una cantidad solicitada de criptomoneda desde la dirección del usuario a la dirección de destino. La transacción parcialmente firmada se firma criptográficamente y una transacción de firma múltiple se transmite a una red de criptomoneda para transferir la cantidad solicitada de criptomoneda desde la dirección del usuario a la dirección de destino (resumen).

1 <https://patentimages.storage.googleapis.com/79/0c/e4/603659579ef05e/US20150324789A1.pdf>

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 4221 de 7 de junio de 2019

Ref. Expediente N° NC2018/0011415

El documento D2² divulga un sistema para implementar al menos una transacción de criptomoneda en un punto de venta mediante el uso de un terminal móvil. El sistema es operable para proporcionar autenticación para implementar la una o más transacciones de criptomoneda, en donde el sistema es operable para enviar al menos una solicitud de autenticación para al menos una transacción de criptomoneda desde un terminal de pago a un servicio de pago alojado a través de uno o más computadores virtuales máquinas, en las que el servicio de pago es operable para proporcionar una solicitud de un código PIN en el terminal móvil; para enviar el código PIN desde el terminal móvil a través de un canal seguro para abrir una bóveda en una o más máquinas virtuales, en donde la bóveda contiene una o más claves privadas (PKI) que se pueden usar para autenticar la al menos una transacción de criptomoneda; y para confirmar la ejecución de al menos una transacción de criptomoneda al menos al terminal de pago (resumen).

5. Examen de Patentabilidad (Art. 14 Decisión 486)

5.1. Novedad (Art 16 Decisión 486)

La reivindicación 1 consiste en: *“Un sistema para proporcionar una verificación de identidad personal multifactorial basada en una cadena de bloques, comprendiendo el sistema (...)”* (Radicado N° NC2018/0011415 el 25 de octubre de 2018).

Tabla 1. Comparación de las características técnicas esenciales, con las del estado de la técnica:

Características esenciales	D1
Uno o varios procesadores de hardware configurados mediante instrucciones legibles por una máquina para: establecer direcciones de verificación en una cadena de bloques	Las direcciones generadas en una rama solo se utilizan para recibir bitcoins. Las direcciones generadas en otra rama solo se utilizan para comprar bitcoins. Las direcciones generadas en la tercera rama solo se utilizan como direcciones de cambio, que reciben las partes no gastadas de las entradas de transacción (Pág. 5, Párr. 0059). La figura 17 muestra un ejemplo del diagrama de bloques funcional (350) del dispositivo seguro (10) y debe entenderse que el dispositivo seguro (10) no está limitado a los componentes y/o disposiciones expuestas en la figura 17. Como se muestra, el diagrama de bloques funcional (350) proporciona una vista simplificada de los circuitos para realizar las funciones del dispositivo seguro (10). El dispositivo seguro (10) puede incluir un interruptor de encendido/apagado (352), un circuito de control de potencia/limitador de corriente (354), una fuente de alimentación fuente (356), y un microprocesador (360) (Pág. 13, Párr. 0158).
Asociación de identificadores con individuos que tienen identidades personales previamente verificadas, estando asociado un primer identificador con un primer individuo, teniendo el primer individuo una identidad personal previamente verificada	Dado que el almacén de datos almacena una de las claves de cifrado, y el servidor almacena una, el usuario aún tiene dos de las tres claves de cifrado necesarias para utilizar esos bitcoins en una transacción incluso a pesar de la pérdida de la tarjeta de bloque (10). Por supuesto, el usuario deberá proporcionar cierta información de identificación (factor de conocimiento) para autorizar el uso de claves de cifrado desde el almacén de datos. En cualquier caso, este seguro a prueba de fallos ayuda a aumentar la seguridad de los conceptos inventivos divulgados actualmente y reduce el riesgo de que el usuario pierda sus bitcoins y su dinero (Pág. 5, Párr. 0060). En el paso (132), el servidor web (56) realiza un primer paso para enviar el nombre de usuario y la contraseña para confirmar la configuración por primera vez. Esto puede incluir un número de serie para un dispositivo seguro particular (10) (Pág. 10, Párr. 0112).
Asignación de direcciones de verificación en una cadena de bloques a los individuos, donde	En la etapa (134), el servidor de cuentas de usuario (52), en respuesta, genera una clave RSA a partir de la contraseña de manera determinista, por ejemplo. El servidor de cuentas de usuario (52)

2 <https://patentimages.storage.googleapis.com/45/35/d4/305693105929de/US20150356555A1.pdf>

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 4221 de 7 de junio de 2019

Ref. Expediente N° NC2018/0011415

una dirección de verificación determinada incluye una clave pública y una clave privada, asignándose una primera dirección de verificación al primer individuo, donde la primera dirección de verificación incluye una primera clave pública y una primera clave privada	almacena una clave pública RSA en la base de datos (54) del dispositivo y envía una clave privada RSA cifrada al usuario con un código de autorización a través del servidor web (56). En el paso (136), el navegador web (82) almacena aún más la clave privada RSA, nuevamente cifrada, con el token de autorización. En la etapa (138), el dispositivo seguro (10) envía un código de autorización que está firmado por la clave privada del dispositivo de usuario (10). El código de autorización se envía al servidor de cuentas de usuario (52), que en la etapa (132) verifica el código de autorización y descifra las claves públicas con El UDEK. Además, el servidor de cuentas de usuario (52) cifra las claves públicas con la clave pública RSA almacenada (Pág. 10, Párr. 0112).
Registro de identificadores y datos biométricos asociados con los individuos en direcciones de verificación correspondientes, donde el primer identificador y los primeros datos biométricos asociados con el primer individuo se registran en la primera dirección de verificación.	El dispositivo seguro (10) puede incluir al menos 3 niveles de seguridad. Una clave privada dentro del dispositivo seguro (10), una clave pública y luego una clave SPK asociada con el escaneo de huellas dactilares del usuario. El navegador (42) de un usuario puede interactuar con Internet (36) en el lado de la red (32), al igual que el correo electrónico y los mensajes de texto SMS, para facilitar las comunicaciones (Pág. 8, Párr. 0094). La base de datos del dispositivo (54) también puede incluir una tabla web que almacena el nombre de una persona que puede definirse como una dirección de correo electrónico para que el usuario fuerce la singularidad, la identificación del dispositivo seguro (10) asociado con la cuenta del usuario, y se incluya una contraseña para verificar la corrección de la contraseña en la tabla web (Pág. 8, Párr. 0098).
Realización de la verificación de identidad personal multifactorial basada en una cadena de bloques utilizando las direcciones de verificación.	Estas claves de cifrado pueden generarse aleatoriamente o pueden derivarse de una clave maestra. Cada clave también puede generar su propia cadena de claves derivadas y esto se conoce como una billetera determinista jerárquica. Dado que la tarjeta de bloque utiliza tres claves de encriptación para asegurar la billetera, una o más de ellas pasan por una cadena determinista. En la realización preferida, en lugar de reducir una rama determinista, reduce tres ramas. Las direcciones generadas en una rama solo se utilizan para recibir bitcoins. Las direcciones generadas en otra rama solo se utilizan para comprar bitcoins. Las direcciones generadas en la tercera rama solo se utilizan como direcciones de cambio, que reciben las partes no gastadas de las entradas de transacción. Al segregar las transacciones de esta manera, la arquitectura de la billetera, como se almacena en la cadena de bloques y sin datos de registro adicionales, puede proporcionar información sobre cuándo y cuántos bitcoins se compraron, cuándo y cuántos bitcoins se recibieron, y cuándo y cuántos bitcoins se enviaron, a la vez que se aislaron los bitcoins que se recibieron de uno mismo como cambio de las partes no gastadas de las transacciones (Pág. 5, Párr. 0059).
Recepción de uno o varios identificadores en relación con una o varias peticiones de verificación de una identidad de uno o varios individuos, donde se recibe el primer identificador en relación con una petición de verificación de una identidad del primer individuo.	1) Para cualquier bitcoin del usuario que posea actualmente, una de las tres claves de cifrado se almacena en la tarjeta de bloque (10). 2) Una de las tres claves de cifrado se almacena en el servidor. 3) Una de las tres claves de cifrado se almacena en el almacén de datos. 4) Cuando el usuario desea enviar bitcoins a otra parte, ya sea un individuo o un comerciante, el usuario hace clic en el botón que está marcado con las marcas de bitcoin, lo que hace que la tarjeta de bloque (10) active la cámara (366) para preparar el escaneo de un código de respuesta rápida (QR) (Pág. 6, Párr. 0062 a 0065). 11) El usuario ingresa la cantidad de bitcoins que desea comprar o la cantidad de moneda fiduciaria que desea convertir, y pasa el dedo por el escáner de huellas dactilares (14) para proporcionar autenticación (Pág. 6, Párr. 0072).
Extracción de los datos biométricos asociados con uno o varios individuos de las direcciones de verificación correspondientes, donde los	6) El usuario pasa el dedo por el escáner de huellas digitales (14) para autorizar la transacción. Los detalles obtenidos del escáner de huellas dactilares (14) se extraen y se envían al servidor para su autenticación. La tarjeta de bloque (10) también firma la transacción utilizando su clave de cifrado almacenada y envía la transacción

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 4221 de 7 de junio de 2019

Ref. Expediente N° NC2018/0011415

primeros datos biométricos asociados con el primer individuo se extraen de la primera dirección de verificación.	firmada al servidor a través del chip (368) del transceptor inalámbrico. Suponiendo que la autorización se basó en los detalles de las huellas dactilares, el servidor completa la transacción firmándola con su clave de cifrado. transmitiendo la transacción firmada conjuntamente a la red Bitcoin, transfiriendo así los bitcoins a su nuevo propietario (Pág. 6, Párr. 0067).
Verificación de la identidad de uno o varios individuos tras recibir datos biométricos y claves privadas coincidentes, donde la identidad personal del primer individuo se verifica tras la recepción de (1) datos biométricos que coinciden con los primeros datos biométricos y (2) una clave privada que coincide con la primera clave privada.	Una realización implica recibir una clave de un solo uso, también conocida como desafío, desde el portal web. Este desafío se puede comunicar a la tarjeta de bloque (10) como datos numéricos simples que el usuario ingresa manualmente usando el teclado (16). El desafío también se puede enviar a la tarjeta de bloque (10) como datos alfanuméricos complejos que se ingresan al escanear un código QR con el código incrustado La cámara o se envía directamente desde el servidor mediante el transceptor inalámbrico incorporado (368). Este desafío se firma con la clave de cifrado integrada y el desafío firmado se puede enviar al servidor para proporcionar un segundo factor de autenticación además del nombre de usuario y la contraseña. ya ingresado en la página de inicio de sesión del portal web, o como un segundo y tercer factor de autenticación si el desafío firmado se envía junto con un escaneo de huellas dactilares para proporcionar la autenticación tanto de posesión como de herencia (Pág. 4, Párr. 0057).

De acuerdo con la tabla anterior, las características esenciales del sistema de la reivindicación 1 habían sido divulgadas previamente en el documento D1, por lo tanto, la materia reivindicada no es nueva.

Asimismo, el documento D1 divulga las características de las reivindicaciones dependientes así:

- Reivindicación 2: Primero, el dispositivo seguro (10) puede cifrar todos sus datos que se envían utilizando una Clave de cifrado de datos de usuario (UDEK). Cualquier dato que permanezca almacenado en el servidor permanece cifrado por este UDEK, aunque el servidor nunca almacena el UDEK. Esto significa que la información solo se puede descifrar cuando se está comunicando con el dispositivo seguro (10). Los datos del usuario y UDEK se combinan y encriptan nuevamente utilizando una clave privada compartida (SPK), que es una clave compartida por el dispositivo seguro (10) y servidor. Este paquete doblemente encriptado puede luego enviarse al servidor a través de un Secure Socket Layer (SSL) que ofrece aún más seguridad en las comunicaciones. El servidor puede usar su copia del SPK para descifrar el paquete y luego puede usar el UDEK para descifrar los datos de usuario necesarios para la transacción específica, incluida la autenticación multifactor enviada con el paquete (Pág. 7, Párr. 0087).
- Reivindicación 3: El servidor de bitcoin wallet también está diseñado para simplificar la contabilidad y la preparación de impuestos. Dado que las transacciones de bitcoin son públicamente visibles en el libro de contabilidad de la cadena de bloques, muchos usuarios generan una nueva clave de cifrado privada, y por lo tanto una nueva dirección de bitcoin pública, para cada transacción, de modo que el saldo completo de su billetera de bitcoin no sea conocido por aquellos con quienes realizan transacciones (Pág. 5, Párr. 0059).
- Reivindicaciones 5, 8 y 9: La generación de direcciones de firma múltiple, descrita anteriormente, puede ser en cualquier forma de "N de M claves" donde $N < M$ y donde N es el número de claves necesarias para firmar la transacción para autorizarla y M es el número total de claves potenciales que se pueden utilizar para firmar la transacción. En la realización preferida, se utilizaron los valores de $N = 2$ y $M = 3$, o se usa un esquema de firma múltiple de 2 de 3, ya que esto brinda

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 4221 de 7 de junio de 2019

Ref. Expediente N° NC2018/0011415

protección contra la pérdida de una sola clave, permite que una clave de recuperación se almacene sin conexión, sin introducir tantas claves como para volverse engorroso, pero también se podría usar un esquema de firma múltiple de 3 de 4 o de 5 de 5 con las claves adicionales almacenadas en servidores adicionales o dispositivos de seguridad adicionales. Si bien las claves adicionales podrían almacenarse en el mismo servidor o en el mismo dispositivo seguro, esto no ofrece ninguna ventaja de seguridad adicional sobre el esquema de firma múltiple 2 de 3, ya que las claves adicionales se pierden al mismo tiempo que el servidor o el dispositivo seguro. están perdidos o comprometidos (Pág. 6, Párr. 0084).

El escáner de huellas dactilares (14) realiza un escaneo de la huella dactilar del usuario, y se pueden utilizar detalles de este escaneo en el método de la presente divulgación. Aunque un escáner de huellas dactilares (14) se describe aquí a modo de ejemplo, se pueden usar otros tipos de lectores biométricos, por ejemplo. Escáner de retina, monitor de frecuencia cardíaca, etc., para proporcionar un mecanismo de verificación al usuario y garantizar que solo los usuarios autorizados de la tarjeta de bloque (10) puedan realizar transacciones (Pág. 4, Párr. 0051).

- Reivindicaciones 6, 7: El escáner de huellas dactilares (14) proporciona otra metodología opcional pero rápida y fácil para proporcionar información de autorización para asegurar la transacción. La combinación de este escaneo de huellas dactilares con un código de acceso ingresado en el teclado (16) proporciona una capa adicional de seguridad al agregar otro factor de autenticación. Un flujo de trabajo bien diseñado significa que el usuario solo necesita realizar tres funciones utilizando las capacidades anteriores para completar una transacción, como una compra de bitcoin. 1) Use la cámara (366) para escanear el código QR que contiene la dirección de bitcoin de destino del comerciante y el monto en dólares. 2) Verifique la cantidad en la pantalla de visualización (12) y, si es correcta, deslice un dedo en el escáner de huellas digitales (14) para autorizar. 3) Espere mientras el sistema de comunicaciones inalámbricas se conecta, transmite la solicitud de transacción al servidor, recibe la transacción inicial, la verifica, la firma y la envía de vuelta al servidor para su firma y transmisión adicionales a la red de bitcoin (Pág. 7, Párr. 0090).
- Reivindicación 10: 1) Para cualquier bitcoin del usuario que posea actualmente, una de las tres claves de cifrado se almacena en la tarjeta de bloque (10). 2) Una de las tres claves de cifrado se almacena en el servidor. 3) Una de las tres claves de cifrado se almacena en el almacén de datos. 4) Cuando el usuario desea enviar bitcoins a otra parte, ya sea un individuo o un comerciante, el usuario hace clic en el botón que está marcado con las marcas de bitcoin, lo que hace que la tarjeta de bloque (10) active la cámara (366) para preparar el escaneo de un código de respuesta rápida (QR) (Pág. 6, Párr. 0062 a 0065). 11) El usuario ingresa la cantidad de bitcoins que desea comprar o la cantidad de moneda fiduciaria que desea convertir, y pasa el dedo por el escáner de huellas dactilares (14) para proporcionar autenticación (Pág. 6, Párr. 0072).

Las reivindicaciones dependientes 2, 3, 5 a 10 tampoco cumplen con el requisito de novedad.

5.2. Nivel Inventivo (Art. 18 Decisión 486)

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 4221 de 7 de junio de 2019

Ref. Expediente N° NC2018/0011415

La reivindicación dependiente 4 consiste en: *“El sistema de acuerdo con la reivindicación 1, donde uno o varios procesadores de hardware están adicionalmente configurados mediante instrucciones legibles por una máquina para proporcionar (...)”* (Radicado N° Radicado No NC2018/0011415 el 25 de octubre de 2018).

Tabla 2. Comparación de las características técnicas esenciales, con las del estado de la técnica:

Reiv.	Características esenciales	D1	D2
1	Ver tabla 1.	Ver tabla 1.	No menciona
4	Una interfaz para la presentación a individuos por medio de plataformas informáticas asociadas, configurándose la interfaz para permitir que un individuo determinado añada o elimine direcciones de verificación asignadas al individuo determinado siempre y cuando se asigne al menos una dirección de verificación al individuo determinado.	No menciona	En la figura 2, se muestra un ejemplo de interfaz de usuario de una aplicación Bitcoin ejecutada en el hardware de computación en un terminal móvil, por ejemplo, un teléfono inteligente. Una interfaz de usuario (UI) (200) es operable para presentar un ejemplo de a quién enviar bitcoins. El US (200) incluye un campo (208) que se usa para ingresar una dirección bitcoin del usuario receptor de bitcoin, e incluye un campo (210) que se emplea para ingresar una cantidad de bitcoins a pagar. Una interfaz de usuario (UI) (202) proporciona una aplicación de usuario de ejemplo que se emplea para solicitar pagos de Bitcoin. Se emplea un campo (206) para mostrar las cantidades de bitcoin solicitadas, y se emplea un campo (205) para ingresar una dirección de la billetera de bitcoin del solicitante. Además, la aplicación de Bitcoin opcionalmente tiene un código QR (204), que opcionalmente un usuario de gastos le lee para obtener direcciones de bitcoin y otra información de manera conveniente (Pág. 7, Párr. 0068).

El documento D1 se considera el estado de la técnica más cercano a la invención definida en la reivindicación de pendiente 4 porque divulga un método en el que se recibe una solicitud cifrada para transferir una cantidad solicitada de criptomoneda desde una dirección de usuario a una dirección de destino. La solicitud incluye una dirección de destino, una cantidad solicitada, una clave de cifrado del dispositivo del usuario y datos biométricos. También se recibe una transacción parcialmente firmada para transferir una cantidad solicitada de criptomoneda desde la dirección del usuario a la dirección de destino. La transacción parcialmente firmada se firma criptográficamente y una transacción de firma múltiple se transmite a una red de criptomoneda para transferir la cantidad solicitada de criptomoneda desde la dirección del usuario a la dirección de destino (resumen).

La diferencia entre la invención definida en la reivindicación dependiente 4 y el sistema divulgado de D1 consiste en una interfaz para la presentación a individuos por medio de plataformas informáticas asociadas, configurándose la interfaz para permitir que un individuo determinado añada o elimine direcciones de verificación asignadas al individuo determinado siempre y cuando se asigne al menos una dirección de verificación al individuo determinado.

El efecto que se logra al incluir una interfaz para la presentación a individuos por medio de plataformas informáticas asociadas, configurándose la interfaz para permitir que un individuo determinado añada o elimine direcciones de verificación asignadas al individuo

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 4221 de 7 de junio de 2019

Ref. Expediente N° NC2018/0011415

determinado siempre y cuando se asigne al menos una dirección de verificación al individuo determinado, es que permite que un usuario definido agregue o elimine la un usuario destinatario teniendo en cuenta una dirección de verificación asignada.

Por lo tanto, el problema técnico objetivo que pretende resolver esta invención se puede formular así: ¿Cómo modificar el sistema conocido en D1 con el fin de permitir a un usuario definido agregar o eliminar un usuario destinatario teniendo en cuenta una dirección de verificación asignada?

Sin embargo, el incluir una interfaz de usuario para permitir a un usuario definido agregar o eliminar un usuario destinatario teniendo en cuenta una dirección de verificación asignada, ya está divulgado en el documento D2 que se refiere a una interfaz de usuario ejecutada en dispositivo computacional (terminal móvil) con campos de editables que permiten realizar el envío de bitcoins, dentro del cual se puede agregar un usuario destinatario mediante una dirección de bitcoin del usuario (Pág. 7, Párr. 0068).

En consecuencia, la persona normalmente versada en la materia, estaría motivada a incluir la interfaz gráfica del documento D2 en el sistema de D1, para así llegar al objeto de la reivindicación dependiente 4. Por lo cual se considera obvia.

6. Conclusión con respecto a novedad y/o nivel inventivo

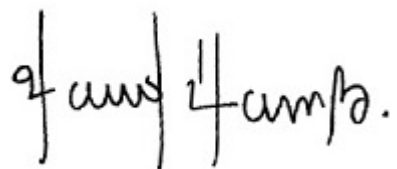
Los requisitos de Patentabilidad de la presente solicitud están afectados así:

Ítem	Documento	Reivindicaciones afectadas	Requisito que afecta
D1	US20150324789	1 a 3, 5 a 10	Novedad
		4	Nivel Inventivo
D2	US20150356555	4	Nivel inventivo

En cumplimiento del artículo 45 de la Decisión 486 de 2000, se le indica que debe dar respuesta dentro del término de sesenta (60) días contados a partir de la fecha de notificación de la presente comunicación. En caso de no dar respuesta al presente requerimiento, o si a pesar de la respuesta subsistieran los impedimentos para la concesión, se denegará la patente.

Si como respuesta a este requerimiento, el solicitante modifica: i) el capítulo reivindicatorio, ii) la descripción de la invención a proteger, iii) o presenta un nuevo capítulo reivindicatorio deberá observar las instrucciones contenidas en el numeral 1.2.2.1.1., del Capítulo Primero del Título X de la Circular Única y la Dirección de Nuevas Creaciones seguirá el procedimiento descrito en el numeral 1.2.2.5.1.

Notifíquese el presente oficio conforme a lo dispuesto en el numeral 6.2 del Capítulo Sexto del Título I de la Circular Única, informándoles que contra el mismo no procede recurso alguno en actuación administrativa.



MARÍA JOSÉ LAMUS BECERRA
DIRECTORA DE NUEVAS CREACIONES

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 4221 de 7 de junio de 2019

Ref. Expediente N° NC2018/0011415

INFORME DE BÚSQUEDA
EXAMEN DE PATENTABILIDAD

Solicitud No.		Examen de patentabilidad							
NC2018/0011415		1°	X	2°		3°		Revoca	
Solicitud Internacional No. (Eliminar toda la fila para solicitudes nacionales) PCT/US2016/024776		Fecha solicitud internacional: (DD/MM/AÑO) 29 de marzo de 2016							
Fecha de determinación estado de la técnica (DD/MM/AÑO) 28/03/2016				Prioridad X		Presentación			
Solicitante BLACK GOLD COIN INC.									
Reivindicaciones que no son objeto de búsqueda por:									
Art. 14	-	Art. 15	-	Art. 20	-	Art. 25 (Falta de unidad de invención)		-	
CRITERIOS DE BÚSQUEDA									
Reivindicaciones objeto de búsqueda				1 a 10					
Palabras clave utilizadas				Block, chain, verification, identity, address, private, public, key, biometric					
Clasificaciones utilizadas para la búsqueda				CIP:	G06F 17/30, G06Q 20/36, G06Q 20/38				
DOCUMENTOS CONSIDERADOS RELEVANTES (Documentos patente, Literatura no patente (LNP): Artículos, catálogos, etc.)									
Informes de búsqueda / Bases de datos consultadas	N° de solicitud de patente / N° de patente / Autor LNP ⁽¹⁾	Fecha de Publicación /Presentación (DD/MM/AAAA)	Reivindicaciones /Secuencias afectadas	Citas relevantes del estado de la técnica				Categoría del documento citado ⁽²⁾	
SIPI	NC2018/0008191	21/08/2018	-	-				E	
	NC2018/0013180	14/12/2018	-	-				E	
	WO2015183901	03/12/2015	-	-				A	
EPO	US2012084563	2012-04-05	-	-				A	
	US2015178693	25/06/2015	-	-				A	
USPTO	US20150324789	12/11/2015	1 a 10	(Pág. 5, Párr. 0059), (Pág. 13, Párr. 0158), (Pág. 5, Párr. 0060), (Pág. 10, Párr. 0112), (Pág. 8, Párr. 0094), (Pág. 8, Párr. 0098), (Pág. 5, Párr. 0059), (Pág. 6, Párr. 0062 a 0065), (Pág. 6, Párr. 0072), (Pág. 6, Párr. 0067), (Pág. 4, Párr. 0057), (Pág. 7, Párr. 0087), (Pág. 6, Párr. 0084), (Pág. 4, Párr. 0051), (Pág. 7, Párr. 0090).				X, Y	
	US20150356555	10/12/2015	1 a 10	(Pág. 7, Párr. 0068).				Y	
Patbase	US2015074409	12/03/2015	-	-				A	
	US2008240420	02/10/2008	-	-				A	
Orbit	US7702739	20/04/2010	-	-				A	
	US20080010685	10/01/2008	-	-				A	
	CN101083530	05/12/2007	-	-				A	
	WO2004010271	29/01/2004	-	-				A	
	US20040168056	26/08/2004	-	-				A	
Googlepatent	JP2005050308	24/02/2005	-	-				A	
	WO2011153539	08/12/2011	-	-				A	
	US5838812	17/11/1998	-	-				A	
	US9094388	28/07/2015	-	-				A	
	US7904360	08/03/2011	-	-				A	
(1) Cita completa literatura no patente (LNP)									

REPÚBLICA DE COLOMBIA

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 4221 de 7 de junio de 2019

Ref. Expediente N° NC2018/0011415

Apellido, A. A. (Fecha). Título del artículo. <i>Nombre de la revista. Volumen</i> (Número), pp-pp.	
O	
Apellido, A. A. (Fecha). Título del artículo. Nombre de la revista. Recuperado de http://xxxxxxx .	
(2) Categorías de documentos citados	
“A” Documento que define el estado general de la técnica no considerado como particularmente relevante. “E” Solicitud de patente o patente anterior pero publicada en la fecha de presentación internacional o en fecha posterior. “L” Documento citado para llamar la atención sobre por ejemplo, dudas acerca de una reivindicación de prioridad o para determinar la fecha de publicación de otra cita, siempre van acompañados de una explicación, por la cual se citan. “O” Documento del tipo actas de conferencia, este tipo de documentos siempre estará acompañado por otra letra que indique la pertinencia del documento, por ejemplo, O,X, O,Y o bien O,A. “P” Documento publicado antes de la fecha de presentación internacional pero con posterioridad a la fecha de prioridad reivindicada.	“T” Documento publicado en fecha posterior a la de presentación o la de prioridad de la solicitud internacional y no entra en conflicto con dicha solicitud, pero puede ser útil para la mejor comprensión del principio o teoría en que se basa la invención, o para demostrar que el razonamiento o los hechos en los que se basa dicha invención son incorrectos. “X” Documento particularmente relevante; la invención reivindicada no puede considerarse nueva o que implique una actividad inventiva por referencia al documento aisladamente considerado. “Y” Documento particularmente relevante; la invención reivindicada no puede considerarse que implique una actividad inventiva cuando el documento se asocia a otro u otros documentos de la misma naturaleza, cuya combinación resulta evidente para un experto en la materia.
Fecha del reporte de búsqueda: 21/05/2019	
Examinador: DIEGO GONZÁLEZ CASTILLO	