

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Resolución N° 60424

Ref. Expediente N° NC2018/0011415

Por la cual se otorga una Patente de Invención

EL SUPERINTENDENTE DE INDUSTRIA Y COMERCIO

en ejercicio de sus facultades legales, en especial de las conferidas en el numeral 26 del artículo 3° del Decreto 4886 de 2011, y

CONSIDERANDO

PRIMERO: Que mediante escrito radicado en esta Superintendencia el 25 de octubre de 2018, con el N° NC2018/0011415, por BLACK GOLD COIN INC., entró a fase nacional la solicitud de patente de invención titulada “SISTEMAS Y MÉTODOS PARA PROPORCIONAR UNA VERIFICACIÓN DE IDENTIDAD PERSONAL MULTIFACTORIAL BASADA EN UNA CADENA DE BLOQUES”, que corresponde a la solicitud internacional PCT/US2016/024776 del 29 de marzo de 2016.

SEGUNDO: Que la solicitud fue publicada en la Gaceta de la Propiedad Industrial N° 846 el 30 de noviembre de 2018, sin que se hubieran presentado oposiciones por parte de terceros.

TERCERO: Que realizado el examen de fondo mediante Oficio N° 4221, notificado el 10 de junio de 2019, se requirió al solicitante en los términos del artículo 45 de la Decisión 486 de la Comisión de la Comunidad Andina para que presentara respuesta a las observaciones de carácter técnico, relacionadas con la patentabilidad o cumplimiento de los requisitos establecidos por esta Decisión para la concesión de la patente.

CUARTO: Que el solicitante mediante escrito radicado bajo el N° NC2018/0011415 el 10 de octubre de 2019, respondió oportunamente el requerimiento formulado y presentó las reivindicaciones 1 a 20 que reemplazan las originalmente presentadas. Es importante señalar que, de acuerdo con las objeciones realizadas en el Oficio N° 4221, relacionadas con el Artículo 34 de la Decisión 486, esta Oficina señala que las objeciones de ampliación de materia son enmendadas, toda vez que se ha establecido que dichas modificaciones hacen referencia a las modificaciones realizadas en etapa internacional y la totalidad de dicha materia se encuentra implícitamente divulgada dentro del documento de presentación nacional. Por lo anterior, se acepta este último capítulo reivindicatorio presentado, comoquiera que se ajusta a las prescripciones contenidas en el artículo 34 de la Decisión 486.

QUINTO: Que en virtud de lo dispuesto en el artículo 14 de la Decisión 486 expedida por la Comisión de la Comunidad Andina “*Los países miembros otorgarán patentes para las invenciones, sean de producto o de procedimiento, en todos los campos de la tecnología, siempre que sean nuevas, tengan nivel inventivo y sean susceptibles de aplicación industrial*”.

SEXTO: Que en el presente caso las reivindicaciones 1 a 20 incluidas en el radicado bajo el N° NC20180011415 el 10 de octubre de 2019, cumplen los requisitos indicados en el considerando anterior, toda vez que refieren sistemas y métodos de verificación de identidad que difiere del estado de la técnica más cercano, US20150324789, en que en el sistema y método no mencionan obtener el identificador almacenado y el hash

Resolución N° 60424

Ref. Expediente N° NC2018/0011415

biométrico almacenado utilizando la dirección de verificación indicada en la petición y firme la verificación de la identidad del individuo como respuesta a una determinación de que el identificador de la petición y los datos biométricos de la petición coinciden con el identificador almacenado y el hash biométrico almacenado, obtener el identificador almacenado y el primer hash biométrico almacenado utilizando la primera dirección de verificación indicada en la petición y 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 provea 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. Adicionalmente, estas diferencias no se encuentran sugeridas en el estado de la técnica y, como consecuencia de ello, se evidencia el efecto 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, implementado un hash de datos biométricos combinados en relación a diferentes parámetros biométricos del usuario, con el fin de aumentar la seguridad al acceso de la información del usuario. Sumado a lo anterior, la materia reivindicada, es susceptible de aplicación industrial.

En consecuencia, las reivindicaciones 1 a 20 cumplen los requisitos de novedad, nivel inventivo y aplicación industrial establecidos en la normatividad citada en precedencia y este Despacho encuentra procedente conceder para las mismas la patente solicitada.

SÉPTIMO: Que de acuerdo con la modificación presentada por el solicitante en el escrito radicado bajo el N° NC20180011415 el 10 de octubre de 2019 y teniendo en cuenta el objeto concedido, se modifica el título de la invención el cual quedará de la siguiente manera: “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”.

Con fundamento en las anteriores consideraciones, el Superintendente de Industria y Comercio,

RESUELVE

ARTÍCULO PRIMERO: Otorgar patente de invención a la solicitud que entró en fase nacional en virtud del Tratado de Cooperación en Materia de Patentes (PCT), para la creación titulada:

“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

Resolución N° 60424

Ref. Expediente N° NC2018/0011415

RELACIÓN CON UN IDENTIFICADOR DE INDIVIDUO E INFORMACIÓN BIOMÉTRICA”

Clasificación IPC: G06F 17/30, G06Q 20/36, G06Q 20/38.

Reivindicación(es): 1 a 20 incluidas en el radicado bajo el N° NC20180011415 el 10 de octubre de 2019, de acuerdo con el anexo 1.

Titular(es): BLACK GOLD COIN INC.

Domicilio(s): 7495 AZURE DRIVE, SUITE 100, LAS VEGAS, NEVADA 89130, 89130, ESTADOS UNIDOS DE AMÉRICA.

Inventores(es): Marcus ANDRADE.

Prioridad(es) N°: 28/03/2016, US (ESTADOS UNIDOS DE AMÉRICA), 15/083,241.

Solicitud internacional N°: PCT/US2016/024776 **Fecha:** 29 de marzo de 2016.

Vigente desde: 29 de marzo de 2016

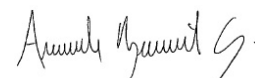
Hasta: 29 de marzo de 2016.

ARTÍCULO SEGUNDO: El titular tendrá los derechos y las obligaciones establecidos en la Decisión 486 de la Comisión de la Comunidad Andina y en las demás disposiciones legales vigentes sobre propiedad industrial, precisando que para mantener vigente la patente se deberá cancelar la tasa anual de mantenimiento, conforme lo dispone el artículo 80 de la referida norma comunitaria.

ARTÍCULO TERCERO: Notificar el contenido de la presente resolución a BLACK GOLD COIN INC, advirtiéndole que contra ella procede el recurso de reposición, ante el Superintendente de Industria y Comercio, el cual podrá ser interpuesto en el momento de la notificación o dentro de los diez (10) días hábiles siguientes a ella.

NOTIFÍQUESE Y CÚMPLASE

Dada en Bogotá D.C., el 5 de noviembre de 2019



ANDRÉS BARRETO GONZÁLEZ
SUPERINTENDENTE DE INDUSTRIA Y COMERCIO

Firmado digitalmente
por: ANDRÉS
BERNARDO BARRETO
GONZALEZ
Fecha: 2019.11.15
18:55:08 COT
Razón: Validez jurídica.
Ubicación: Bogotá,
Colombia.



Resolución N° 60424

Ref. Expediente N° NC2018/0011415

ANEXO 1

REIVINDICACIONES CONCEDIDAS

1. Un sistema (100) para proporcionar una verificación de la identidad personal multifactorial basada en una cadena de bloques, comprendiendo el sistema:

uno o varios medios de almacenamiento (124) legibles por una computadora (104) configurados para almacenar una cadena de bloques;

un sistema informático del lado del servidor (102) que comprende uno o varios procesadores programados para ejecutar instrucciones de un programa informático que, cuando se ejecutan, hacen que el sistema informático del lado del servidor:

asigne una dirección de verificación (110) asociada con la cadena de bloques a un individuo, teniendo el individuo una identidad personal previamente verificada;

almacene, en uno o varios medios de almacenamiento legibles por una computadora, un identificador del individuo (108) y un *hash* biométrico del individuo en asociación con la dirección de verificación (112) asociada con la cadena de bloques,

siendo el *hash* biométrico es un *hash* de datos biométricos del individuo y

donde cada uno del identificador, el *hash* biométrico, y la dirección de verificación son diferentes entre sí y diferentes de las claves privadas y públicas de las cuales se derivó la dirección de verificación;

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

obtenga el identificador almacenado y el *hash* biométrico almacenado utilizando la dirección de verificación indicada en la petición; y

firmar la verificación de la identidad del individuo como respuesta a una determinación de que el identificador de la petición y los datos biométricos de la petición coinciden con el identificador almacenado y el *hash* biométrico almacenado.

2. El sistema de acuerdo con la reivindicación 1, en el cual se hace que el sistema informático del lado del servidor firme, utilizando la clave privada a partir de la cual se derivó la dirección de verificación, la verificación de la identidad del individuo como respuesta a la determinación de que el identificador de la petición y los datos biométricos de la petición coinciden con el identificador almacenado y el *hash* biométrico almacenado.

3. El sistema de acuerdo con la reivindicación 2, en el cual se hace que el sistema informático del lado del servidor:



Resolución N° **60424**

Ref. Expediente N° NC2018/0011415

almacene, en uno o varios medios de almacenamiento legibles por una computadora, la clave privada en asociación con la dirección de verificación asociada con la cadena de bloques;

obtenga, desde el dispositivo del lado del cliente, la clave privada en relación con la petición de verificación de la identidad del individuo;

obtenga la clave privada almacenada utilizando la dirección de verificación indicada en la petición; y

firmes, utilizando la clave privada, la verificación de la identidad del individuo como respuesta a una determinación de que el identificador de la petición, los datos biométricos de la petición y la clave privada de la petición coinciden con el identificador almacenado, el *hash* biométrico almacenado, y la clave privada almacenada.

4. El sistema de acuerdo con la reivindicación 3, en el cual se almacena también la clave privada en el dispositivo del lado del cliente, y en el cual el dispositivo del lado del cliente es un dispositivo de usuario del individuo.

5. El sistema de acuerdo con la reivindicación 1, en el cual se hace que el sistema informático del lado del servidor:

asigne otra dirección de verificación asociada con la cadena de bloques al individuo;

almacene, en uno o varios medios de almacenamiento legibles por una computadora, otro *hash* biométrico del individuo en asociación con la otra dirección de verificación asociada con la cadena de bloques, donde el otro *hash* biométrico es un *hash* de otros datos biométricos del individuo;

obtenga, desde el dispositivo del lado del cliente, los otros datos biométricos en relación con la petición de verificación de la identidad del individuo, indicando adicionalmente la petición la otra dirección de verificación asociada con la cadena de bloques;

obtenga el otro *hash* biométrico almacenado utilizando la otra dirección de verificación indicada en la petición; y

firmes la verificación de la identidad del individuo como respuesta a una determinación de que el identificador de la petición, los datos biométricos de la petición, los otros datos biométricos de la petición coinciden con el identificador almacenado, el *hash* biométrico almacenado, y el otro *hash* biométrico almacenado.

6. El sistema de acuerdo con la reivindicación 5, en el cual se hace que el sistema informático del lado del servidor:

obtenga, a través de una interfaz de usuario, un comando iniciado por el usuario para añadir la otra dirección de verificación como una dirección de la cadena de bloques para el individuo; y



Resolución N° 60424

Ref. Expediente N° NC2018/0011415

asigne la otra dirección de verificación asociada con la cadena de bloques al individuo basándose en el comando iniciado por el usuario.

7. El sistema de acuerdo con la reivindicación 5, en el cual se hace que el sistema informático del lado del servidor:

obtenga, a través de una interfaz de usuario, un comando iniciado por el usuario para eliminar la otra dirección de verificación como una dirección de la cadena de bloques para el individuo; y

desasocie la otra dirección de verificación asociada con la cadena de bloques del individuo basándose en el comando iniciado por el usuario.

8. El sistema de acuerdo con la reivindicación 1, en el cual se hace que el sistema informático del lado del servidor:

proporcione 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 dirección de verificación asociada con la cadena de bloques, donde se le brinda acceso al primer usuario a los datos almacenados basándose en la verificación en cuanto a que el primer usuario tiene una primera clave privada, donde la primera clave privada es diferente de la clave privada de la cual se derivó la dirección de verificación; y

niegue el acceso, a un segundo usuario, que no es el individuo, a los datos almacenados basándose en la verificación de que el segundo usuario tiene una segunda clave privada.

9. El sistema de acuerdo con la reivindicación 1, en el cual los datos biométricos comprenden una imagen, un registro o un patrón.

10. El sistema de acuerdo con la reivindicación 1, en el cual los datos biométricos están relacionados con una huella digital, venas palmares, reconocimiento facial, ADN, huella palmar, geometría de la mano, reconocimiento del iris, retina, olor, andares o con la voz.

11. Un sistema para proporcionar una verificación de la identidad personal multifactorial basada en una cadena de bloques, comprendiendo el sistema:

uno o varios medios de almacenamiento legibles por una computadora configurados para almacenar una cadena de bloques;

un sistema informático del lado del servidor que comprende uno o varios procesadores programados para ejecutar instrucciones de un programa informático que, cuando se ejecutan, hacen que el sistema informático del lado del servidor:

asigne múltiples direcciones de verificación de la cadena de bloques al individuo (204), teniendo el individuo una identidad personal previamente verificada, las múltiples direcciones de verificación incluyen una primera dirección de verificación asociada con la cadena de bloques y una segunda dirección de verificación asociada con la cadena de bloques;

Resolución N° **60424**

Ref. Expediente N° NC2018/0011415

almacene, en uno o varios medios de almacenamiento legibles por una computadora, (i) un identificador del individuo y un primer *hash* biométrico del individuo en asociación con la primera dirección de verificación asociada con la cadena de bloques y (ii) un segundo *hash* biométrico del individuo en asociación con la segunda dirección de verificación asociada con la cadena de bloques (206),

donde el primer *hash* biométrico es un *hash* de los primeros datos biométricos del individuo, y el segundo *hash* biométrico es un *hash* de segundos datos biométricos del individuo, y

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 (304);

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 (304); y

firmes, 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 (306);

proporcione 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.

12. Un método para proporcionar una verificación de la identidad personal multifactorial basada en una cadena de bloques, implementándose el método mediante un sistema informático del lado del servidor que comprende uno o



Resolución N° **60424**

Ref. Expediente N° NC2018/0011415

varios procesadores que ejecutan instrucciones de un programa informático que, cuando se ejecutan, llevan a cabo el método, comprendiendo el método:

el almacenamiento, por el sistema informático del lado del servidor, de una cadena de bloques en uno o varios medios de almacenamiento legibles por una computadora del sistema informático del lado del servidor;

la asignación (204), por el sistema informático del lado del servidor, de una dirección de verificación asociada con la cadena de bloques a un individuo, teniendo el individuo una identidad personal previamente verificada;

el almacenamiento (206), por el sistema informático del lado del servidor, en uno o varios medios de almacenamiento legibles por una computadora, de un identificador del individuo y un *hash* biométrico del individuo en asociación con la dirección de verificación asociada con la cadena de bloques,

donde el *hash* biométrico es un *hash* de datos biométricos del individuo, y donde cada uno de los siguientes: el identificador, el *hash* biométrico y la dirección de verificación son diferentes entre sí y son diferentes de las claves privadas y públicas de las cuales se derivó la dirección de verificación;

la obtención (304), por el sistema informático del lado del servidor, desde el dispositivo del lado del cliente, del identificador y los datos biométricos en relación con una petición de verificación de la identidad del individuo, indicando la petición la dirección de verificación asociada con la cadena de bloques;

la obtención, por el sistema informático del lado del servidor, del identificador almacenado y del *hash* biométrico almacenado utilizando la dirección de verificación indicada en la petición (304); y

la asignación, por el sistema informático del lado del servidor, de la verificación de la identidad del individuo (306) como respuesta a una determinación en cuanto a que el identificador de la petición y los datos biométricos de la petición coinciden con el identificador almacenado y con el *hash* biométrico almacenado.

13. El método de acuerdo con la reivindicación 12, que comprende la firma, por el sistema informático del lado del servidor, utilizando la clave privada de la cual se derivó la dirección de verificación, de la verificación de la identidad del individuo como respuesta a la determinación en cuanto a que el identificador de la petición y los datos biométricos de la petición coinciden con el identificador almacenado y con el *hash* biométrico almacenado (306).

14. El método de acuerdo con la reivindicación 13, que comprende:

el almacenamiento, por el sistema informático del lado del servidor, en uno o varios medios de almacenamiento legibles por una computadora, de la clave privada en asociación con la dirección de verificación asociada con la cadena de bloques;

la obtención, por el sistema informático del lado del servidor, desde el dispositivo del lado del cliente, de la clave privada en relación con la petición de verificación de la identidad del individuo;



Resolución N° **60424**

Ref. Expediente N° NC2018/0011415

la obtención de la clave privada almacenada utilizando la dirección de verificación indicada en la petición; y

la firma, por el sistema informático del lado del servidor, utilizando la clave privada, de la verificación de la identidad del individuo como respuesta a una determinación en cuanto a que el identificador de la petición, los datos biométricos de la petición, y la clave privada de la petición coinciden con el identificador almacenado, con el *hash* biométrico almacenado, y con la clave privada almacenada.

15. El método de acuerdo con la reivindicación 12, que comprende:

la asignación, por el sistema informático del lado del servidor, de otra dirección de verificación asociada con la cadena de bloques al individuo;

el almacenamiento, por el sistema informático del lado del servidor, en uno o varios medios de almacenamiento legibles por una computadora, de otro *hash* biométrico del individuo en asociación con la otra dirección de verificación asociada con la cadena de bloques, donde el otro *hash* biométrico es un *hash* de otros datos biométricos del individuo;

la obtención, por el sistema informático del lado del servidor, desde el dispositivo del lado del cliente, de los otros datos biométricos en relación con la petición de verificación de la identidad del individuo, indicando además la petición la otra dirección de verificación asociada con la cadena de bloques;

la obtención, por el sistema informático del lado del servidor, del otro *hash* biométrico almacenado utilizando la otra dirección de verificación indicada en la petición; y

la firma, por el sistema informático del lado del servidor, de la verificación de la identidad del individuo como respuesta a una determinación en cuanto a que el identificador de la petición, los datos biométricos de la petición, los otros datos biométricos de la petición coinciden con el identificador almacenado, con el *hash* biométrico almacenado, y con el otro *hash* biométrico almacenado.

16. El método de acuerdo con la reivindicación 13, que comprende:

la obtención, por el sistema informático del lado del servidor, a través de una interfaz de usuario, de un comando iniciado por el usuario para añadir la otra dirección de verificación como una dirección de la cadena de bloques para el individuo; y

la asignación, por el sistema informático del lado del servidor, de la otra dirección de verificación asociada con la cadena de bloques al individuo basándose en el comando iniciado por el usuario.

17. El método de acuerdo con la reivindicación 13, que comprende:

la obtención, por el sistema informático del lado del servidor, a través de una interfaz del usuario, de un comando iniciado por el usuario para eliminar la otra dirección de verificación como una dirección de la cadena de bloques para el individuo; y



Resolución N° 60424

Ref. Expediente N° NC2018/0011415

la desasociación, por el sistema informático del lado del servidor, de la otra dirección de verificación asociada con la cadena de bloques del individuo basándose en el comando iniciado por el usuario.

18. El método de acuerdo con la reivindicación 12, que comprende:

la provisión, por el sistema informático del lado del servidor, a un primer usuario, que no es el individuo, del acceso a los datos almacenados en uno o varios medios de almacenamiento legibles por una computadora en asociación con la dirección de verificación asociada con la cadena de bloques, proporcionándole al primer usuario acceso 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 dirección de verificación; y

la negación, por el sistema informático del lado del servidor, a un segundo usuario, que no es el individuo, del acceso a los datos almacenados basándose en la verificación de que el segundo usuario tiene una segunda clave privada.

19. El método de acuerdo con la reivindicación 12, en el cual los datos biométricos comprenden una imagen, un registro o un patrón.

20. El método de acuerdo con la reivindicación 12, en el cual los datos biométricos están relacionados con una huella digital, venas palmares, reconocimiento facial, ADN, huella palmar, geometría de la mano, reconocimiento del iris, retina, olor, andares o con la voz.

