

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 13203 de 25 de junio de 2026

Ref. Expediente N° NC2023/0010374

Señores
ARCULUS HOLDINGS, LLC

TÍTULO DE LA SOLICITUD: “DISPOSITIVOS, SISTEMAS Y MÉTODOS PARA AUTENTICACIÓN DE CLAVE PÚBLICA O PRIVADA”

NUMERO DE SOLICITUD INTERNACIONAL: PCT/US2022/011660

FECHA DE PRESENTACIÓN INTERNACIONAL: 7 de enero de 2022

PRIORIDADES: 8/01/2021, US (ESTADOS UNIDOS DE AMÉRICA), 63/135,157
25/10/2021, US (ESTADOS UNIDOS DE AMÉRICA), 63/271,545

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

Revisada la modificación a la solicitud objeto de estudio, la cual fue radicada el 6 de octubre de 2023 bajo el número NC2023/0013380, y teniendo en cuenta lo señalado en el artículo 34 de la Decisión 486 de 2000 de la Comisión de la Comunidad Andina, esta oficina acepta las modificaciones presentadas por ajustarse a los requisitos legales.

2. Objeto de la invención

El problema planteado consiste en la necesidad de brindar seguridad ante ataques informáticos realizados a transacciones firmadas y difundidas por la red, donde la clave privada almacenada electrónicamente en un monedero digital conectado a internet es vulnerable.

Para resolver dicho problema técnico, la solicitud en estudio plantea la firma de las transacciones en un entorno no conectado a internet, o almacenamiento en frío, donde la transacción se firma digitalmente fuera de línea antes de transmitirse a la red, el elemento seguro del dispositivo de almacenamiento mantiene las claves y realiza las operaciones criptográficas internamente.

3. Reivindicaciones estudiadas

El presente estudio se basa en el capítulo reivindicatorio presentado el 6 de octubre de 2023.

4. De la solicitud de patente

4.1. Reivindicaciones

Teniendo en cuenta lo establecido en el artículo 30 de la Decisión 486 de 2000 de la Comisión de la Comunidad Andina:

Oficio N° 13203 de 25 de junio de 2026

Ref. Expediente N° NC2023/0010374

"Las reivindicaciones definirán la materia que se desea proteger mediante la patente. Deben ser claras y concisas y estar enteramente sustentadas por la descripción. (...)"

Esta oficina informa que, la estructura del pliego reivindicatorio no permite identificar con claridad el objeto a proteger y las características que lo definen. Se recomienda presentar cada reivindicación conservando la estructura: "Preámbulo - enlace gramatical - parte característica". El preámbulo indica cuál es el objeto de la invención, que suele coincidir con el título de la invención (aparato, proceso, composición, etc.) y las características técnicas conocidas en el estado de la técnica. De otro lado, la parte caracterizante comprende los elementos técnicos y/o procedimentales que en conjunto con el preámbulo se desean proteger y que distinguen la invención de las del estado de la técnica. Estas dos partes están separadas por el enlace gramatical "caracterizado por", "comprendido por", "que comprende", "que consiste" o "que contiene". Adicionalmente, se debe tener en cuenta que las reivindicaciones deben ir numeradas consecutivamente, preferiblemente por números arábigos.

Esta oficina informa que, el término "*signo*" (Reiv. 1, 19, 39) no es reconocido en el campo técnico descrito y parece corresponder con un error en la traducción del término "sign" o "firma". Se sugiere realizar las aclaraciones o correcciones correspondientes.

Esta oficina informa que, el capítulo reivindicatorio no es claro, toda vez que, la reivindicación 38 parece corresponder con una reivindicación dependiente de la reivindicación 37, sin embargo, su dependencia no se encuentra especificada. Ahora bien, en el caso de ser independiente, corresponde a una selección de características sin una relación funcional, se sugiere aclarar o hacer las modificaciones correspondientes. Asimismo, la expresión "*el sistema está configurado además para comprar o intercambiar criptomonedas*" (Reiv. 5) sugiere materia no patentable. Se sugiere eliminar.

Esta oficina informa que, en el capítulo reivindicatorio persisten los errores en las dependencias de las reivindicaciones, por lo que se sugiere revisar y ajustar las dependencias del pliego reivindicatorio, toda vez que las reivindicaciones dependientes 22, 35 y 36 hacen referencia a las reivindicaciones 17-19, 19-34 y 19-35, respectivamente; sin embargo, esto implica que hacen referencia a más de una reivindicación independiente, impidiendo identificar claramente las modalidades que reclama, generando un número excesivo de modalidades e impidiendo comparar la materia reivindicada con el estado de la técnica, por lo cual se sugiere ajustar las dependencias del capítulo reivindicatorio para que cada reivindicación dependiente haga referencia a solo una reivindicación independiente.

Esta oficina informa que, el pliego reivindicatorio no es conciso, toda vez que las reivindicaciones 1, 19, 31, 37 y 39 se encuentran reclamando las mismas características técnicas, lo cual no permite establecer una diferencia considerable entre las reivindicaciones independientes, sugiriendo que el solicitante reclame la protección de la misma materia varias veces. Se recomienda colocar, de manera razonablemente general, las características esenciales de las dos reivindicaciones en una reivindicación independiente y los elementos específicos particulares o alternativos dentro de una reivindicación dependiente a esta.

En consecuencia, es necesario que allegue las aclaraciones o modificaciones correspondientes para dar cumplimiento a lo establecido en el citado artículo.

Oficio N° 13203 de 25 de junio de 2026

Ref. Expediente N° NC2023/0010374

5. Determinación del Estado de la Técnica

La fecha para determinar el estado de la técnica es el 8 de enero de 2021, 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	US 2019/0325408	“Devices, systems, and methods for securing, accessing and transacting cryptocurrency and non-cryptocurrency assets”	24 de octubre de 2019
D2	US 10,102,510	“Method and system of conducting a cryptocurrency payment via a mobile device using a contactless token to store and protect a user’s secret key”	16 de noviembre de 2018

D1¹ divulga un (...) sistema para transacciones seguras de información, que incluye un dispositivo informático con una aplicación de software instalada y configurado para almacenar una clave pública de criptomoneda, y un dispositivo de cifrado de hardware configurado para almacenar una clave privada de cifrado, y configurado para conectarse selectivamente en la comunicación de datos al dispositivo informático para firmar una transacción de criptomoneda. El dispositivo informático transmite una transacción firmada recibida del dispositivo de cifrado de hardware para la verificación de la transacción (Resumen).

D2² divulga un (...) método y un sistema para realizar pagos con criptomonedas a través de un dispositivo móvil, utilizando un token sin contacto para almacenar y proteger la clave secreta del usuario. El dispositivo móvil recibe del token una billetera de criptomonedas cifrada con la clave secreta. El dispositivo recibe una instrucción de pago, solicitando las credenciales del usuario para su aprobación. En respuesta, el dispositivo envía al token un mensaje que contiene la billetera cifrada, la instrucción de pago y las credenciales del usuario. Utilizando la clave secreta, el token descifra la billetera de criptomonedas y crea una transacción de pago firmando digitalmente la instrucción y transmitiéndola a una red o plataforma de intercambio de criptomonedas. La confirmación de la transacción requiere un PIN, datos biométricos o huella dactilar en el dispositivo móvil, o bien autenticación mediante botón, PIN o huella dactilar en el token (Resumen).

6. Examen de Patentabilidad

De acuerdo con lo establecido en el artículo 14 de la Decisión 486 de 2000 de la Comisión de la Comunidad Andina, en el cual se establecen los requisitos de patentabilidad objeto de la solicitud en estudio, esta Oficina presenta a continuación el análisis de los requisitos de patentabilidad.

6.1. Novedad

Teniendo en cuenta lo señalado en el artículo 16 de la Decisión 486 de 2000 de la Comisión de la Comunidad Andina, la reivindicación independiente 1 (NC2023/0013380 del 6 de octubre de 2023) refiere a: “Un sistema para realizar una transacción, que comprende: (...)”. A continuación, se presenta la tabla comparativa entre el objeto reivindicado y los documentos encontrados en el estado de la técnica:

¹<https://worldwide.espacenet.com/patent/search?q=pn%3DUS2019325408A1>
²<https://worldwide.espacenet.com/patent/search?q=pn%3DUS10102510B2>



Oficio N° 13203 de 25 de junio de 2026

Ref. Expediente N° NC2023/0010374

CARACTERÍSTICAS ESENCIALES	D1	D2
Un sistema para realizar una transacción, que comprende:	(...) Sistema para transacciones seguras de criptomonedas (Párr. 8).	(...) El sistema está programado para proporcionar un método para realizar un pago con criptomonedas a través de un dispositivo informático móvil que comprende, utilizando el dispositivo informático móvil, almacenar una billetera cifrada recibida de un token de seguridad portátil que está separado del dispositivo móvil (Párr. 400).
Un dispositivo de almacenamiento, teniendo el dispositivo de almacenamiento un circuito integrado que comprende:	(...) El dispositivo de cifrado de hardware (22) está codificado con instrucciones ejecutables que, al ser ejecutadas por un procesador, se pueden utilizar (...) (Párr. 24)	(...) Un dispositivo de tarjeta de token (1102) que comprende una memoria programada para almacenar un valor secreto (1104) (Párr. 406).
Al menos un primer elemento seguro, teniendo el primer elemento seguro un procesador, una memoria digital.	(...) El dispositivo de cifrado de hardware (22) genera y almacena la clave privada en un microcontrolador seguro (elemento seguro) (...) El dispositivo de cifrado de hardware (22) incluye una carcasa (41), una pantalla táctil (40), uno o más elementos de autenticación biométrica (42) y un puerto (24) que proporciona una conexión física entre el dispositivo de cifrado de hardware (22) y un teléfono inteligente u otro dispositivo informático (26) (Párr. 26)	(...) un token que incluye almacenamiento de tokens para guardar credenciales de usuario privadas, un sistema de comunicaciones de tokens y un procesador de tokens que proporciona funciones criptográficas (Párr. 55).
Una primera interfaz de comunicaciones de campo cercano (NFC).	(...) El dispositivo de cifrado de hardware (22) no tiene ningún puerto y utiliza protocolos de transferencia de datos inalámbricos como BLUETOOTH®, comunicación de campo cercano (NFC), Wi-Fi™, ZIGBEE® o cualquier otro protocolo relacionado para firmar las transacciones (Párr. 35).	(...) La recepción de la billetera cifrada desde el token de seguridad portátil y el envío del mensaje al token de seguridad portátil utilizan la comunicación de campo cercano (NFC) (Párr. 403).
El primer módulo de memoria digital de elemento seguro que incorpora instrucciones legibles por el primer procesador de elemento seguro para hacer que el primer elemento seguro almacene una clave pública y una clave privada en estados cifrados en la memoria digital.	(...) El dispositivo de cifrado de hardware (22) contiene las claves privadas del usuario almacenadas en un elemento seguro EAL5+. Las claves nunca salen de dicho elemento (Párr. 35). En el estado de la técnica se encuentra implícito que los elementos seguros tipo EAL5+ incluyen algoritmos hash como parte de su funcionalidad en seguridad criptográfica.	(...) El dispositivo de tarjeta de token (1102) recibe una instrucción de “generar billetera”, genera una billetera ECDSA (1112), cifra la billetera 1112 con el secreto interno (1104) y transmite la billetera cifrada (como un “blob”) con una clave pública al dispositivo informático móvil (1106) (Párr. 439). (...) El token NFC es un token sin contacto que admite las especificaciones de Java Card y GlobalPlatform. Preferiblemente, el token cuenta con un alto nivel de aprobación de seguridad según los esquemas Common Criteria y/o FIPS (Párr. 168) (...) El token está diseñado para admitir múltiples applets de Java Card (Párr. 169). Se encuentra implícito en el estado de la técnica que, el token NFC comprende un



Genere una clave pública. Usar la clave privada. Realizar operaciones de signo y hash.	(...) Los elementos de procesamiento dentro del dispositivo de cifrado de hardware (22) están preprogramados con la clave pública de firma de código que se utiliza para verificar que el firmware descargado sea un producto compatible y autorizado antes de que se ejecute dicho firmware (Párr. 39). (...) la aplicación busca la clave privada correspondiente en el dispositivo de cifrado de hardware (22) para firmar la transacción (Párr. 45).	elemento seguro, ya que cumple con las especificaciones de Java Card Applet. (...) El dispositivo de tarjeta de token (1102) recibe una instrucción de "generar billetera", genera una billetera ECDSA (1112), cifra la billetera (1112) con el secreto interno (1104) y transmite la billetera cifrada (como un "blob") con una clave pública al dispositivo informático móvil (1106) (Párr. 439). (...) El dispositivo de tarjeta token (1102) puede firmar transacciones (como las que utiliza BITCOIN) mediante ECDSA (Párr. 415) (...) El dispositivo de tarjeta de token (1102) también almacena una copia del secreto (1114), o una versión hash del mismo, para permitir la verificación (Párr. 420) (...) El número de identificación personal (PIN) (1105) se almacena únicamente en el dispositivo de tarjeta de token (1102), en formato hash u otro formato seguro (Párr. 420) (...) Firma digital: función=función de firma digital; autorización=clave de firma privada; parámetro=hash del mensaje; salida=firma digital sobre el hash del mensaje (Párr. 38).
Un dispositivo de procesamiento que tiene una interfaz de usuario. Una segunda interfaz NFC. Una interfaz de comunicación configurada para la conexión a una red de comunicaciones global. Teniendo el dispositivo de procesamiento una memoria digital y un procesador, la memoria digital del dispositivo de procesamiento programada con	(...) El dispositivo de cifrado de hardware (22) está conectado a un teléfono inteligente u otro dispositivo informático inteligente (26), ya sea a través de un puerto de conexión físico (24) o mediante un método de conectividad inalámbrica como BLUETOOTH®, Wi-Fi™, NFC, ZIGBEE® o cualquier otro protocolo de comunicaciones inalámbricas (Párr. 51) (...) Dispositivos informáticos (26), (38) pueden acoplarse opcionalmente a una pantalla para mostrar información (...) La conexión con el teléfono inteligente (26) puede realizarse mediante conexiones inalámbricas (como BLUETOOTH® u otros protocolos inalámbricos estándar o personalizados) o a través de un cable integrado o separado (Párr. 21) (...) El disco duro del teléfono inteligente (26) y el dispositivo de cifrado de hardware (22) están codificados con instrucciones ejecutables que, al ser ejecutadas por un procesador (en cada dispositivo), hacen que este realice las acciones descritas en las figuras 2, 4 y 5. En un ejemplo de implementación, el usuario	(...) Un dispositivo informático móvil (1106) programado con una aplicación (1108) que contiene una biblioteca de almacenamiento seguro (1110) (Párr. 408). (...) en su aplicación móvil (1108), y se le indica que deslice su dispositivo de tarjeta token (1102); la aplicación (1108) genera una instrucción de "generar billetera" que se emite utilizando la interfaz NFC (Párr. 439). (...) La instrucción de pago con criptomonedas se recibe mediante uno de los siguientes métodos: una interfaz de programación de aplicaciones (API) de intercambio de criptomonedas, uno o más mensajes de comunicación de campo cercano (NFC) y acceso a Internet celular o inalámbrico (Párr. 402). (...) En cada dispositivo móvil, existe una única instancia del Servicio Hoverkey que acepta solicitudes de la aplicación y, cuando se requiere una contraseña, el Servicio Hoverkey recupera la contraseña en nombre de la aplicación mediante una serie de intercambios con el applet de Java



Oficio N° 13203 de 25 de junio de 2026

Ref. Expediente N° NC2023/0010374

instrucciones legibles por el dispositivo de procesamiento procesador para hacer que el dispositivo de procesamiento establezca una conexión a través de NFC con la interfaz NFC del primer elemento seguro. Para enviar información al primer elemento seguro para su procesamiento por el primer elemento seguro. Para establecer una interfaz de usuario operable para acceder a una red de transacciones a través de la red global de comunicaciones.	interactúa con el teléfono inteligente (26) para acceder a la interfaz gráfica de usuario mediante una aplicación web que se ejecuta en un navegador web móvil o una aplicación móvil (comúnmente llamada "app") instalada en el teléfono inteligente (26) y mostrada en la pantalla (30). La aplicación instalada en el teléfono inteligente (26) se comunica y envía/recibe datos desde/hacia el dispositivo de cifrado de hardware (22) cuando el conector del dispositivo (24) está insertado y en comunicación de datos con el teléfono inteligente (26), a través del conector (32) del teléfono inteligente (Párr. 24) (...) El usuario decide a qué dirección enviar los fondos, que puede introducirse en la interfaz de usuario que se muestra en la pantalla (30) del teléfono inteligente (26), con o sin el dispositivo de cifrado de hardware (22) conectado (...) La verificación de la transacción es recibida por la aplicación instalada en el teléfono inteligente (26), paso (210). El dispositivo de cifrado de hardware (22) puede estar en comunicación de datos con el teléfono inteligente (26) durante toda la transacción, o puede ser opcionalmente desconectado o separado del teléfono inteligente (26) después de que este envíe la autorización al teléfono inteligente (Párr. 25) (...) la confirmación de la transacción se envía a la aplicación de criptomonedas en el teléfono inteligente u otro dispositivo informático inteligente (26), y luego los parámetros de la transacción se comunican a una cadena de bloques para el registro de la transacción (Párr. 50).	Card a través de la interfaz NFC (Párr. 127). (...) Un token NFC/Bluetooth proporciona entonces una clave asimétrica al teléfono, que a su vez se autentica ante un servicio de terceros mediante la realización de una firma digital dentro del propio teléfono. (Párr. 10). (...) El dispositivo móvil (1106) transmite la billetera cifrada (1112), las instrucciones de pago y el PIN al dispositivo de tarjeta token (1102) (Párr. 456). (...) La aplicación móvil (1108) se conecta a una red de criptomonedas (1150), como la red BITCOIN (blockchain), a través del ordenador del usuario (1140), o a través de una plataforma de intercambio de criptomonedas (1120) o un banco BITCOIN (por ejemplo, COINBASE) (Párr. 443).
En donde las instrucciones legibles por el procesador del dispositivo de almacenamiento y el procesador del dispositivo de procesamiento, cuando las leen los procesadores respectivos, son capaces de hacer que el sistema realice los pasos de: (a) el dispositivo de procesamiento recibe	(...) El usuario decide a qué dirección enviar los fondos, que puede ingresar en la interfaz de usuario que se muestra en la pantalla (30) del teléfono inteligente (26), con o sin el dispositivo de cifrado de hardware (22) conectado. La aplicación instalada en el teléfono inteligente (26) recibe al usuario la dirección de criptomoneda de destino y la cantidad de fondos que se enviarán a esa dirección, paso (202) (Párr. 25).	(...) instrucciones ejecutables por máquina que pueden descargarse e instalarse en el dispositivo informático móvil (1106) o en el firmware del dispositivo de tarjeta token (1102). (Párr. 425). (...) El usuario hace clic en el botón "pagar con criptomonedas" en una página web que contiene una dirección de billetera de criptomonedas. Alternativamente, el usuario puede ingresar los parámetros de la transacción manualmente directamente en la aplicación (1108) (Párr. 461).



Oficio N° 13203 de 25 de junio de 2026

Ref. Expediente N° NC2023/0010374

el inicio de una transacción a través de la interfaz de usuario.		
(b) el dispositivo de procesamiento que establece la conexión con el primer elemento seguro a través de NFC.	(...) El dispositivo de cifrado de hardware (22) no tiene ningún puerto y utiliza protocolos de transferencia de datos inalámbricos como BLUETOOTH®, comunicación de campo cercano (NFC), Wi-Fi™, ZIGBEE® o cualquier otro protocolo relacionado para firmar las transacciones. La aplicación del teléfono inteligente (26) detecta automáticamente el entorno del dispositivo de cifrado de hardware (22). Si se encuentra el dispositivo de cifrado de hardware (22) (o la clave de hardware), solicita confirmación para ingresar a la siguiente capa de autenticación, como el sensor biométrico o la contraseña (Párr. 35).	(...) El servicio Hoverkey recupera la contraseña en nombre de la aplicación mediante una serie de intercambios con el applet de Java Card a través de la interfaz NFC (Párr. 127).
(c) el dispositivo de procesamiento envía información al primer elemento seguro para su procesamiento a través del enlace NFC.		(...) El dispositivo móvil (1106) transmite el monedero cifrado (1112), las instrucciones de pago y el PIN al dispositivo de la tarjeta token (1102) (Párr. 456).
(d) el primer elemento seguro recupera la clave privada, realiza operaciones hash utilizando la clave privada para definir una firma, verificando una cadena asociada con la clave pública para confirmar que la firma se ajusta a una firma de clave pública que solo podría haberse generado usando la clave privada específica, firmar la transacción y enviar información de la transacción firmada al dispositivo de procesamiento.	(...) El sistema incluye un dispositivo informático con una aplicación de software instalada, configurado para almacenar una clave pública de criptomoneda. Además, incluye un dispositivo de cifrado de hardware configurado para almacenar una clave privada de cifrado de criptomoneda, configurado para conectarse selectivamente al dispositivo informático para la comunicación de datos y la firma de una transacción de criptomoneda (Párr. 8) (...) Confirmar que una clave de cifrado privada generada por el dispositivo de cifrado de hardware coincide con una clave pública de criptomoneda en una aplicación residente en el dispositivo de computación inteligente; solicitar uno o más parámetros de transacción al dispositivo de cifrado de hardware, (...) comparar las credenciales biométricas del solicitante con una clave de cifrado privada para confirmar la transacción de criptomonedas y generar una transacción de criptomonedas firmada (Reiv. 27).	(...) El dispositivo de tarjeta token (1102) autentica al usuario comparando el PIN introducido con el PIN almacenado (1105), descifra la cartera (1112) utilizando la clave secreta interna (1104), firma la instrucción de pago con la cartera descifrada y genera una transacción de criptomoneda. A continuación, el dispositivo de tarjeta token (1102) transmite la instrucción de pago firmada al dispositivo informático móvil (1106) y desecha la cartera (1112) (Párr. 457) (...) Firma digital: función=función de firma digital, autorización simple=clave de firma privada; parámetro=hash del mensaje; salida=firma digital en el hash del mensaje (Párr. 37)
(e) el dispositivo de procesamiento establece una sesión de comunicación a través de la red de comunicaciones global con un servidor de intercambio de la red de transacciones y envía la información de la transacción firmada al servidor de intercambio para iniciar la transacción.	El dispositivo informático transmite la transacción firmada recibida del dispositivo de cifrado de hardware para su verificación (Párr. 8) Inicia la transmisión de la transacción de criptomoneda firmada a una red de criptomonedas para su verificación por parte de un ordenador minero, la ejecución de la transacción firmada deseada y la escritura de la transacción en una cadena de bloques (Párr. 54).	(...) El dispositivo informático móvil (1106) reenvía la transacción a la red de criptomonedas (1150) a través del intercambio de criptomonedas (1120) o directamente a través del ordenador personal (1140) (Párr. 463).



Oficio N° 13203 de 25 de junio de 2026

Ref. Expediente N° NC2023/0010374

De acuerdo con la comparación realizada anteriormente se concluye que la materia de la reivindicación 1 no es nueva.

Así mismo, D1 divulga las características de las reivindicaciones dependientes de la siguiente manera:

- Reivindicación 2: (...) El sistema utiliza una (...) una billetera fría. Las billeteras o claves privadas se pueden generar y almacenar en la aplicación del teléfono inteligente (26) o en el dispositivo de cifrado de hardware (22). El usuario puede transferir los activos de criptomonedas entre la billetera caliente (con la clave privada almacenada en la aplicación) y la billetera fría (con la clave privada almacenada en el dispositivo de cifrado de hardware 22) (Párr. 44).

- Reivindicación 3: (...) La transacción se realiza utilizando la firma de clave privada del dispositivo de cifrado de hardware (22). Una vez completada, se envía la confirmación de la transacción a la aplicación de criptomoneda en el teléfono inteligente u otro dispositivo informático inteligente (26), y los parámetros de la transacción se comunican a la cadena de bloques para su registro (Párr. 50).

- Reivindicación 4: (...) el usuario decide a qué dirección enviar los fondos, que puede introducirse en la interfaz de usuario que se muestra en la pantalla (30) del teléfono inteligente (26), con o sin el dispositivo de cifrado de hardware (22) conectado. La aplicación instalada en el teléfono inteligente (26) recibe al usuario la dirección de criptomoneda de destino y la cantidad de fondos que se enviarán a esa dirección, paso (202) (Párr. 25).

- Reivindicaciones 5 a 8: (...) NFC, BLUETOOTH®, W-Fi™ y ZIGBEE®) para realizar pagos directamente. Por ejemplo, el dispositivo de cifrado de hardware (22) se puede configurar para comunicarse directamente (de igual a igual) con los dispositivos de punto de venta (POS) del comercio u otros dispositivos informáticos. Los usuarios utilizan métodos de autenticación biométrica o códigos de acceso para autenticarse y enviar transacciones para el uso diario (Párr. 37).

- Reivindicaciones 9 y 10: (...) Dispositivo (26) al que está conectado el dispositivo de cifrado de hardware (22). El puerto de conexión (24) puede variar según el tipo de teléfono inteligente u otro dispositivo móvil que se utilice junto con el dispositivo (Párr. 28).

- Reivindicación 14: (...) El dispositivo de cifrado de hardware (22) puede realizar transacciones de forma independiente. El dispositivo de cifrado de hardware (22) cuenta con todos los protocolos de comunicación inalámbrica necesarios (como NFC, Bluetooth®, Wi-Fi™ y Zigbee®, entre otros) para realizar pagos directamente (Párr. 37) (...) La conexión inalámbrica habilita realizar pagos sin contacto utilizando una o más criptomonedas desde el dispositivo de cifrado de hardware (Reiv. 33).

- Reivindicaciones 16 y 17: (...) La confirmación de la clave pública de la criptomoneda inicia la autenticación adicional del usuario y la transacción de criptomoneda o la actividad de acceso al sistema deseada por el usuario a través de elementos de autenticación biométrica en el paso (530). El dispositivo de cifrado de hardware (22) solicita la interacción del usuario a través de la pantalla (40) y realiza uno o más escaneos de huellas dactilares, retina, reconocimiento de voz o reconocimiento facial, como se indicó anteriormente, para capturar las credenciales biométricas del usuario (Párr. 52) (...) En el paso (540), se procesan las credenciales biométricas del usuario para confirmar una transacción de criptomonedas, el acceso a una cuenta o registros en línea, el acceso al

Oficio N° 13203 de 25 de junio de 2026

Ref. Expediente N° NC2023/0010374

sistema de votación u otra actividad. Si las credenciales biométricas se confirman, el proceso (500) continúa con la ejecución de la actividad deseada por el usuario (Párr. 53).

- Reivindicación 18: (...) el que el dispositivo de cifrado de hardware se conecta al dispositivo informático inteligente mediante una conexión inalámbrica entre ambos (Reiv. 22) (...) la conexión inalámbrica es una conexión de comunicación de campo cercano (NFC) (Reiv. 25).

Así mismo, D2 divulga las características de las reivindicaciones dependientes de la siguiente manera:

- Reivindicación 2: (...) Un sistema informático programado para proporcionar almacenamiento seguro de criptomonedas. En general, el sistema de la figura 11 está programado para configurar, en un dispositivo móvil como un teléfono inteligente, una billetera cifrada con una clave secreta conocida únicamente por un dispositivo de tarjeta token independiente, pero que puede verificarse tanto por la tarjeta token como por una aplicación del teléfono inteligente si el PIN ingresado en el dispositivo de tarjeta token es correcto. En consecuencia, el teléfono inteligente que almacena la billetera cifrada resulta inútil si es robado (Párr. 399) El dispositivo y el token pueden realizar una autenticación criptográfica mutua antes de la transmisión de la autorización cifrada (Párr. 52) (...) dado que las claves privadas de Bitcoin de los usuarios se almacenan en un dispositivo de seguridad de hardware dedicado, que puede ser una tarjeta inteligente o un dispositivo portátil, y que generalmente no está conectado a internet, es relativamente seguro contra malware, incluidos virus, troyanos y registradores de pulsaciones de teclas (Párr. 397).

- Reivindicación 4: (...) El dispositivo de tarjeta token (1102) recibe una instrucción de “generar billetera”, genera una billetera ECDSA (1112), la cifra con el secreto interno (1104) y la transmite (como un “blob”) junto con una clave pública al dispositivo informático móvil (1106). En algunas implementaciones, la billetera (1112) puede ser cualquier tipo de billetera de criptomonedas o clave de criptomonedas (...) 3. El dispositivo informático móvil (1106) almacena el blob y la clave pública, y muestra la clave pública al usuario. (Párr. 441 - 442).

- Reivindicación 5: (...) El usuario hace clic en el botón “pagar con criptomonedas” en una página web que contiene la dirección de una billetera de criptomonedas (Párr. 461) (...) El dispositivo informático móvil (1106) reenvía la transacción a la red de criptomonedas (1150) a través del intercambio de criptomonedas (1120) (Párr. 463).

- Reivindicaciones 6 a 10: (...) 1. El comerciante ordena al terminal de punto de venta (TPV) (1130) que cobre al usuario un importe específico en criptomoneda por un producto o servicio determinado (...) 2. El TPV (1130) ordena al usuario que acerque su dispositivo móvil (1106) a un terminal NFC conectado al TPV (...) 3. El dispositivo móvil (1106) recibe una instrucción NFC y, en respuesta, abre la aplicación (1108) u otra aplicación de pago que pueda realizar las funciones descritas (...) 4. La aplicación (1108) muestra: Nombre del comerciante (+ clave pública); Producto; Importe (...) 5. El usuario autoriza la transacción. Se le solicita que introduzca un PIN. También se puede utilizar la autenticación biométrica en lugar del PIN; por lo tanto, todas las referencias al uso de un PIN en este documento se refieren a la autorización biométrica como alternativa. 6. El usuario introduce el PIN, que la aplicación (1108) almacena temporalmente, y se le indica que deslice el lector de tarjetas (1102) (...) 7. El dispositivo móvil (1106) transmite la cartera cifrada (1112), la instrucción de pago y el PIN al lector de tarjetas (1102) (...) 8. El lector de tarjetas (1102) autentica al usuario comparando el PIN introducido con el PIN almacenado (1105), descifra la cartera (1112) utilizando la clave secreta interna (1104), firma la instrucción de pago con la cartera descifrada y realiza una transacción de

Oficio N° 13203 de 25 de junio de 2026

Ref. Expediente N° NC2023/0010374

criptomonedas. A continuación, el lector de tarjetas (1102) transmite la instrucción de pago firmada al dispositivo móvil (1106) y desecha la cartera (1112) (...) 9. El dispositivo móvil (1106) puede transmitir la transacción al comercio mediante NFC o directamente a su banco mediante una conexión de datos en red (Párr. 450 - 458).

- Reivindicaciones 11, 13 y 14: (...) El token NFC es un token sin contacto que admite las especificaciones Java Card y GlobalPlatform. Preferiblemente, el token cuenta con un alto nivel de certificación de seguridad según los estándares Common Criteria y/o FIPS. El producto inicial se implementa en el formato ISO 7810 (tarjeta de crédito) (Párr. 168). La comunicación entre el token y el dispositivo móvil utiliza NFC, aunque también podrían emplearse otros canales, como Bluetooth, Bluetooth Low Energy (BLE) u otros tipos de comunicación por radiofrecuencia. Asimismo, se contemplan tokens que requieren contacto con el dispositivo móvil, como tarjetas de banda magnética y tarjetas de contacto electrónicas (Párr. 83).

- Reivindicaciones 12 y 15: (...) Normalmente, el token será una tarjeta inteligente sin contacto, aunque también serían posibles otros tokens que la persona lleve consigo. Entre los tokens adecuados se incluyen un anillo para llevar en el dedo, un dispositivo incorporado a un reloj, cinturón, gafas, ropa o cualquier otro objeto que el usuario suela llevar, o incluso un dispositivo implantado bajo la piel del usuario. El token puede tener botones, áreas sensibles al tacto u otros medios para permitir la retroalimentación/entrada manual o de otro tipo por parte del usuario a través del token (Párr. 81) (...) En el estado de la técnica se encuentra implícito que las tarjetas NFC comprenden metal, toda vez que su principio de funcionamiento es por inducción electromagnética, particularmente, comprendiendo en sus antenas metales como cobre o aluminio.

- Reivindicaciones 16 y 17: (...) La confirmación de que la credencial del usuario coincide con un identificador de autenticación registrado en el token de seguridad portátil se realiza mediante PIN, datos biométricos o huella dactilar en el dispositivo móvil, o mediante confirmación por pulsación de botón, PIN o huella dactilar en el token de seguridad portátil. La billetera puede contar con protección de integridad y cifrado (Párr. 400) (...) El identificador de autenticación puede ser un número de identificación personal (PIN) o un identificador biométrico como una huella dactilar. En una implementación, la recepción de la billetera cifrada se produce al enviar, al token de seguridad portátil, una solicitud de cifrado que integra la billetera de criptomonedas (Párr. 401) (...) El usuario autoriza la transacción. Se le solicita que ingrese un PIN. También se puede utilizar la autenticación biométrica en lugar de un PIN; por lo tanto, todas las referencias al uso de un PIN en este documento se refieren a permitir el uso de la autenticación biométrica como alternativa (Párr. 454).

- Reivindicación 18: (...) Mensajería segura mediante NFC (...) La especificación de la Plataforma Global (GP) admite el intercambio seguro de mensajes APDU entre la tarjeta y el terminal. GP admite tres niveles de seguridad de mensajería: 1. Autenticación de entidad únicamente (...) 2. (1) anterior más protección de integridad (...) 3. (2) anterior más protección de confidencialidad (...) Hoverkey L1 admite mensajería segura de nivel 3 mediante el Protocolo de Canal Seguro GP versión 2 (SCP02) (Párr. 207-211).

Las reivindicaciones dependientes 2 a 18 tampoco cumplen con el requisito de novedad.

Por otro lado, partiendo de la falta de concisión mencionada previamente para el grupo de reivindicaciones 1, 19, 31, 37 y 39, es importante indicar que, teniendo en cuenta que las características técnicas incluidas dentro de dichas reivindicaciones ya habían sido anticipadas por los documentos D1 y D2, de acuerdo con el análisis comparativo de las

Oficio N° 13203 de 25 de junio de 2026

Ref. Expediente N° NC2023/0010374

reivindicaciones 1 a 18, las reivindicaciones 19, 20, 22 a 27, 29 y 30 carecen de novedad, teniendo en cuenta que D1 enseña que (...) las transacciones son firmadas por el dispositivo de cifrado de hardware (22) a través de una API en la que la aplicación envía la transacción solicitada para su firma al dispositivo (22) (...) el dispositivo (22) firma la transacción con la clave privada integrada del usuario y devuelve la transacción firmada a la aplicación para su envío a la cadena de bloques (Párr. 38) (...) el firmware del dispositivo de cifrado de hardware (22) está firmado con una clave privada de firma de código. Los elementos de procesamiento dentro del dispositivo de cifrado de hardware (22) están preprogramados con la clave pública de firma de código (Párr. 39) y D2 enseña que (...) el dispositivo de tarjeta token (1102) autentica al usuario comparando el PIN introducido con el PIN almacenado (1105), descifra la billetera (1112) utilizando el secreto interno (1104), firma la instrucción de pago con la billetera descifrada y genera una transacción de criptomoneda. A continuación, el dispositivo de tarjeta token (1102) transmite la instrucción de pago firmada al dispositivo informático móvil (1106) y descarta la billetera (1112) (Párr. 457). Por lo tanto, las reivindicaciones 19 a 30 no son nuevas

Por otro lado, partiendo de la falta de concisión mencionada previamente para el grupo de reivindicaciones 1, 19, 31, 37 y 39, es importante indicar que, teniendo en cuenta que las características técnicas incluidas dentro de dichas reivindicaciones ya habían sido anticipadas por los documentos D1 y D2, de acuerdo con el análisis comparativo de las reivindicaciones 1 a 18, las reivindicaciones 31 a 36 carecen de novedad, teniendo en cuenta que D1 enseña que (...) el dispositivo informático transmite la transacción firmada recibida del dispositivo de cifrado de hardware para su verificación (Párr. 8) Inicia la transmisión de la transacción de criptomoneda firmada a una red de criptomonedas para su verificación por parte de un ordenador minero, la ejecución de la transacción firmada deseada y la escritura de la transacción en una cadena de bloques (Párr. 54) y D2 enseña que (...) la transacción de pago con criptomonedas se transmite a la red de criptomonedas mediante la comunicación con uno de los siguientes dispositivos: un ordenador independiente propiedad del usuario del dispositivo móvil, un terminal del comercio o una plataforma de intercambio de criptomonedas (Párr. 406) (...) El lector de tarjetas (1102) autentica al usuario comparando el PIN introducido con el PIN almacenado (1105), descifra la cartera (1112) utilizando la clave secreta interna (1104), firma la instrucción de pago con la cartera descifrada y realiza una transacción de criptomonedas. A continuación, el lector de tarjetas (1102) transmite la instrucción de pago firmada al dispositivo móvil (1106) y desecha la cartera (1112) (Párr. 457). Por lo tanto, las reivindicaciones 31 a 36 no son nuevas.

Teniendo en cuenta lo señalado en el artículo 16 de la Decisión 486 de 2000 de la Comisión de la Comunidad Andina, la reivindicación independiente 37 (NC2023/0013380 del 6 de octubre de 2023) refiere a: *“Un dispositivo de autenticación, teniendo el dispositivo un circuito integrado que comprende (...)”*. A continuación, se presenta la tabla comparativa entre el objeto reivindicado y los documentos encontrados en el estado de la técnica:

CARACTERÍSTICAS ESENCIALES	D1	D2
Un dispositivo de autenticación, teniendo el dispositivo un circuito integrado que comprende	(...) Un dispositivo de cifrado de hardware configurado para almacenar una clave de cifrado de criptomoneda privada, y está configurado para conectarse selectivamente en la comunicación de datos al dispositivo informático para firmar una transacción de criptomoneda (Párr. 8).	(...) un dispositivo de seguridad portátil (por ejemplo, una tarjeta inteligente sin contacto o una pulsera), junto con un secreto que el usuario pueda recordar fácilmente (por ejemplo, un código PIN) (Párr. 2).



Oficio N° 13203 de 25 de junio de 2026

Ref. Expediente N° NC2023/0010374

Al menos un primer elemento seguro, teniendo el primer elemento seguro un procesador, una memoria digital y una interfaz de comunicaciones de campo cercano (NFC).	(...) El dispositivo de cifrado de hardware (22) genera y almacena la clave privada en un microcontrolador seguro (elemento seguro) (Párr. 26) (...) El dispositivo de cifrado de hardware (22) no tiene ningún puerto y utiliza protocolos de transferencia de datos inalámbricos como BLUETOOTH®, comunicación de campo cercano (NFC), Wi-Fi™, ZIGBEE® o cualquier otro protocolo relacionado para firmar las transacciones (Párr. 35).	(...) El dispositivo de tarjeta de token (1102) recibe una instrucción de “generar billetera”, genera una billetera ECDSA (1112), cifra la billetera (1112) con el secreto interno (1104) y transmite la billetera cifrada (como un “blob”) con una clave pública al dispositivo informático móvil (1106) (Párr. 439). (...) El token NFC es un token sin contacto que admite las especificaciones de Java Card y GlobalPlatform. Preferiblemente, el token cuenta con un alto nivel de aprobación de seguridad según los esquemas Common Criteria y/o FIPS (Párr. 168) (...) El token está diseñado para admitir múltiples applets de Java Card (Párr. 169). Se encuentra implícito en el estado de la técnica que, el token NFC comprende un elemento seguro, ya que cumple con las especificaciones de Java Card Applet.
Comprendiendo el primer elemento seguro de memoria digital un módulo que incorpora instrucciones legibles por el procesador del primer elemento seguro para hacer que el primer elemento seguro almacene un código de autenticación en la memoria digital.	(...) El elemento seguro utilizado en el dispositivo de cifrado de hardware (22) también se comunica a través de un bus SPI protegido mediante TLS únicamente con el procesador ARM (...) Durante el proceso de inicialización del dispositivo de cifrado de hardware (22) en la fabricación, el procesador ARM genera una clave aleatoria única que se envía al elemento seguro. Este almacena la clave y, a partir de ese momento, exige que todos los mensajes transmitidos a través del bus SPI estén firmados con dicha clave inmutable. Esto protege contra ataques en los que el elemento seguro se extrae del dispositivo de cifrado de hardware (22) original y se coloca en otra llave de hardware para intentar eludir la autenticación biométrica (Párr. 41) (...) Incluir la firma de la transacción firmada transmitida con una segunda clave privada de acuerdo con un proceso de autenticación de multifirma (Párr. 31).	(...) La autenticación del dispositivo puede ser completamente independiente de la autenticación del token (Párr. 45) (...) el token puede operar en modo de factor único, que descifra la autorización tras la autenticación mutua con el dispositivo. (Párr. 46) (...) Se puede ejecutar un servicio en el dispositivo móvil que controla las funciones criptográficas del dispositivo y el acceso al recurso. Se puede ejecutar un applet en el token que proporciona las funciones criptográficas del token (Párr. 47) (...) El applet implementa: El proceso de activación (también conocido como «personalización» en la terminología común de tarjetas inteligentes), que incluye: (...) Emparejamiento dispositivo/token (...) Generación de la clave de cifrado de contraseña (PEK) (...) Configuración inicial del PIN del usuario (...) El protocolo de autenticación mutua criptográfica (Párr. 181 -186)
Transmita la información de autenticación a un dispositivo móvil en respuesta a la recepción de una comunicación desde el dispositivo móvil vinculado a través de un enlace de comunicaciones con el primer elemento seguro a través de la interfaz NFC, la	(...) El usuario confirma la transacción mediante una coincidencia exitosa de huella digital, momento en el que el dispositivo de cifrado de hardware (22) firma la transacción con la clave privada integrada del usuario y devuelve la transacción firmada a la aplicación para su envío a la cadena de bloques (Párr. 38) (...) La aplicación es la principal puerta de enlace para interactuar con las redes de criptomonedas. Esta aplicación funciona como una billetera de criptomonedas multi-token y se utiliza para enviar y recibir monedas. En	(...) la comunicación entre el token y el dispositivo móvil utiliza NFC, (...) un sistema para autenticar el acceso a un recurso informático en un dispositivo móvil mediante un token de seguridad portátil comprende: (...) un dispositivo que incluye un recurso informático a proteger, un sistema de comunicación y almacenamiento para guardar la autorización cifrada del recurso (...) un token que incluye almacenamiento para guardar las credenciales privadas del usuario, un sistema de comunicación y un procesador que proporciona



Oficio N° 13203 de 25 de junio de 2026

Ref. Expediente N° NC2023/0010374

información relativa a una transacción.	general, recibir criptomonedas no requiere la conexión del dispositivo de cifrado de hardware (22) (...) la aplicación busca la clave privada correspondiente en el dispositivo de cifrado de hardware (22) para firmar la transacción. La autenticación mediante smartphone se utiliza para desbloquear el dispositivo de cifrado de hardware (22) y autorizar al propietario. Se puede introducir un código PIN en el dispositivo como método de autenticación de respaldo (Párr.45).	funciones criptográficas (...) durante su uso, la autorización cifrada almacenada en el dispositivo se transmite al token mediante el sistema de comunicación, se descifra en el token utilizando las credenciales del usuario, el token genera, al menos parcialmente, una respuesta de desbloqueo, que el sistema de comunicación transmite de forma segura al dispositivo móvil mediante dicha respuesta (...) el dispositivo está configurado para desbloquear el recurso si la respuesta recibida es válida. (Párr. 83- 87) (...) El sistema incorpora un software para tarjetas inteligentes programado para generar monederos de criptomonedas y firmar transacciones (...) la autenticación segura mediante huella dactilar utiliza PIN o contraseñas más largas (...) El dispositivo de tarjeta token (1102) puede firmar transacciones (como las utilizadas por Bitcoin) mediante ECDSA (Párr. 415-416)
---	---	---

De acuerdo con la comparación realizada anteriormente se concluye que la materia de la reivindicación 37 no es nueva.

Así mismo, D1 divulga las características de la reivindicación dependiente de la siguiente manera:

- Reivindicación 38: (...) Monedero frío (con la clave privada almacenada en el dispositivo de cifrado de hardware (22)). De esta forma, el usuario puede tener una pequeña cantidad de criptomoneda en el monedero caliente para transacciones rápidas y, al mismo tiempo, transferir los fondos al dispositivo de cifrado de hardware (22) (monedero de hardware) para mayor seguridad (Párr. 44).

Así mismo, D2 divulga las características de la reivindicación dependiente de la siguiente manera:

- Reivindicación 38: (...) El sistema de la figura 11 está programado para utilizar la infraestructura descrita en secciones anteriores, con un software de tarjeta inteligente programado para admitir la generación de monederos de criptomonedas y la firma de transacciones (...) la compatibilidad con huella digital segura utiliza PIN o contraseñas más largas (...) está programado para admitir las siguientes funciones: 1. El dispositivo de tarjeta token (1102) puede firmar transacciones (como las utilizadas por Bitcoin) mediante ECDSA. (Párr. 415-416).

La reivindicación dependiente 38 tampoco cumple con el requisito de novedad.

Por otro lado, partiendo de la falta de concisión mencionada previamente para los grupos de reivindicaciones 1, 19, 31, 37 y 39, es importante indicar que, teniendo en cuenta que las características técnicas incluidas dentro de dichas reivindicaciones ya habían sido anticipadas por los documentos D1 y D2, de acuerdo con el análisis comparativo de las reivindicaciones 1 a 38, la reivindicación 39 carece de novedad, teniendo en cuenta que D1 enseña que (...) en cualquier transacción y almacenamiento de criptomonedas (como Bitcoin u otras criptomonedas distintas de Bitcoin, conocidas colectivamente como



Oficio N° 13203 de 25 de junio de 2026

Ref. Expediente N° NC2023/0010374

Altcoins), se requiere una clave privada y una clave pública para completar la transacción. La clave pública es similar a un número de cuenta que facilita la transferencia de fondos. La clave privada se mantiene confidencial y se utiliza para autorizar pagos salientes (por ejemplo, enviar fondos a otras cuentas) (Párr. 3) (...) El dispositivo de cifrado de hardware (22) está firmado con una clave privada de firma de código. Los elementos de procesamiento dentro del dispositivo de cifrado de hardware (22) están preprogramados con la clave pública de firma de código que se utiliza para verificar (Párr. 39) (...) La confirmación final de la transacción se realiza mediante la firma de clave privada del dispositivo de cifrado de hardware (22). Una vez hecho esto, la confirmación de la transacción se envía a la aplicación de criptomoneda en el teléfono inteligente u otro dispositivo informático inteligente (26), y los parámetros de la transacción se comunican a una cadena de bloques para su registro (Párr. 50) y D2 enseña que (...) un token que incluye almacenamiento para guardar credenciales privadas del usuario, un sistema de comunicación y un procesador que proporciona funciones criptográficas (...) y en el que, durante su uso, el sistema de comunicación del dispositivo transmite una autorización cifrada al token; esta se descifra en el token utilizando las credenciales del usuario; el token genera, al menos parcialmente, una respuesta de desbloqueo, la cual se transmite de forma segura al dispositivo móvil mediante el sistema de comunicación; se requiere que el usuario se autentique por separado en el dispositivo móvil; y se desbloquea el recurso si tanto la respuesta de desbloqueo requerida como la autenticación por separado son válidas (Párr. 57-58) (...) El dispositivo de tarjeta token (1102) autentica al usuario comparando el PIN introducido con el PIN almacenado (1105), descifra la cartera (1112) utilizando la clave secreta interna (1104), firma la instrucción de pago con la cartera descifrada y genera una transacción de criptomoneda. A continuación, el dispositivo de tarjeta token (1102) transmite la instrucción de pago firmada al dispositivo informático móvil (1106) y desecha la cartera (1112) (Párr. 457). Por lo tanto, la reivindicación 39 no es nueva.

Así mismo, D1 divulga las características de la reivindicación dependiente de la siguiente manera:

- Reivindicación 40: (...) sistema para transacciones seguras de criptomonedas, que incluye un dispositivo informático con una aplicación de software instalada y configurado para almacenar una clave pública de criptomoneda. Además, incluye un dispositivo de cifrado de hardware configurado para almacenar una clave privada de cifrado de criptomoneda (Párr. 8) (...) aplicación almacenada en ella para gestionar la ejecución de la transacción de criptomonedas (Reiv. 14) (...) realizar una amplia gama de transacciones de criptomonedas, como se muestra en la FIG. 4B. Por lo tanto, el usuario puede utilizar la aplicación para acceder a múltiples elementos de menú y seleccionar una pluralidad de funciones y configuraciones para realizar transacciones de criptomonedas (Párr. 48) (...) El dispositivo de cifrado de hardware (22) ofrece un rendimiento óptimo en combinación con una aplicación móvil que proporciona un ecosistema integrado para el usuario final. La aplicación es la principal puerta de enlace para interactuar con las redes de criptomonedas. Esta aplicación funciona como una billetera de criptomonedas multi-token y se utiliza para enviar y recibir monedas (Párr. 45) (...) definir una dirección de destinatario, un tipo de criptomoneda y una cantidad de criptomoneda para la transacción de criptomoneda, en respuesta a una solicitud de parámetros de transacción del dispositivo informático inteligente (Reiv. 14).

Así mismo, D2 divulga las características de la reivindicación dependiente de la siguiente manera:

- Reivindicación 40: (...) El sistema está programado para proporcionar un método para realizar un pago con criptomonedas a través de un dispositivo informático móvil que

Oficio N° 13203 de 25 de junio de 2026

Ref. Expediente N° NC2023/0010374

comprende, mediante el dispositivo informático móvil, almacenar una billetera cifrada recibida de un token de seguridad portátil que está separado del dispositivo móvil, donde la billetera cifrada comprende una billetera de criptomonedas cifrada con una clave secreta que está restringida al token de seguridad portátil; mediante el dispositivo informático móvil, recibir una instrucción de pago con criptomonedas; mediante el dispositivo informático móvil, solicitar una credencial de usuario para aprobar la instrucción de pago con criptomonedas; mediante el dispositivo informático móvil, enviar, al token de seguridad portátil, un mensaje en respuesta a la recepción de la credencial de usuario, donde el mensaje comprende la billetera cifrada, la instrucción de pago con criptomonedas y la credencial de usuario; y donde el envío del mensaje hace que el token de seguridad portátil: descifre, utilizando la clave secreta, la billetera de criptomonedas de la billetera cifrada; en respuesta a la confirmación de que la credencial de usuario coincide con un identificador de autenticación registrado con el token de seguridad portátil, cree una transacción de pago con criptomonedas firmando digitalmente la instrucción de pago con criptomonedas utilizando la billetera de criptomonedas; transmita la transacción de pago con criptomonedas a una red de criptomonedas o banco o intercambio de criptomonedas; y borre la billetera de criptomoneda (Párr. 400).

La reivindicación dependiente 40 tampoco cumple con el requisito de novedad.

7. Conclusión

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

Ítem	Documento	Reivindicaciones afectadas	Requisito que afecta
D1	US 2019/0325408	1 a 40	Novedad
D2	US 10,102,510	1 a 40	Novedad

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 el 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 de esta Superintendencia. De igual forma, deberá tener presente que de conformidad con el literal a) del numeral 1.2.2.5.1. de la norma ibidem, será necesario acreditar el pago de la tasa por concepto de modificación a solicitudes en trámites, de conformidad con el valor establecido en la resolución de tasas vigentes.

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.



Sandra Isabel Calderon Rodriguez



Oficio N° **13203** de **25 de junio de 2026**

Ref. Expediente N° NC2023/0010374

DIRECTORA DE NUEVAS CREACIONES (E)



Oficio N° 13203 de 25 de junio de 2026

Ref. Expediente N° NC2023/0010374

INFORME DE BÚSQUEDA
EXAMEN DE PATENTABILIDAD

Solicitud No.				Examen de patentabilidad							
NC2023/0010374				1°	X	2°	-	3°	-	Revoca	-
Solicitud Internacional No.				Fecha solicitud internacional: (DD/MM/AÑO)							
PCT/US2022/011660				7 de enero de 2022							
Fecha de determinación estado de la técnica (DD/MM/AÑO)						Prioridad			Presentación		
08/01/2021						X			-		
Solicitante											
ARCULUS HOLDINGS, LLC											
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 40					
Palabras clave utilizadas						cryptocurrency transaction, blockchain transaction, cold storage, hardware wallet, secure element, private key, public key, NFC, digital signature, hash operation, authentication code, encrypted key, payment module, card reader, transaction server.					
Clasificaciones utilizadas para la búsqueda						CIP:		G06Q 20/06, G06Q 20/32, G06Q 20/34, 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		NC2021/0018107		29/12/2021		-		-			A
		NC2021/0008982		04/08/2023		-		-			A
USPTO / ISA / EPO / CNIPA		US2019/0325408		24/10/2019		1 a 40		Resumen, Párr. 3, 8, 21, 24, 25, 26, 28, 31, 35, 37, 38, 39, 41, 44, 45, 48, 50, 51, 52, 53, 54; Reiv. 14, 22, 25, 27, 33.			X
		US2016/0261411		08/09/2016		-		-			A
JPO		WO2019/218055		21/11/2019		-		-			A
		WO2020/049951		12/03/2020		-		-			A
Patbase		US10102510		16/10/2018		1 a 40		Resumen, Párr. 2, 10, 37, 38, 45, 46, 47, 52, 55, 57-58, 83, 83-87, 127, 168, 169, 181-186, 207-211, 397, 399, 400, 401, 402, 403, 406, 408, 415, 415-416, 420, 425, 439, 441-442, 443, 450-458, 454, 456, 457, 461, 463.			X
		US2020226332		16/07/2020		-		-			A
		US2019164156		30/05/2019		-		-			A
		US2021049591		18/02/2021		-		-			A
Orbit		EP3826225		26/05/2021		-		-			A
		EP3794491		24/03/2021		-		-			A
		EP3717998		07/10/2020		-		-			A
Origin		CA3044991		02/12/2019		-		-			A
		RU190666U		08/07/2019		-		-			A



Oficio N° 13203 de 25 de junio de 2026

Ref. Expediente N° NC2023/0010374

	WO2020204749	08/10/2020	-	-	A
(1) Cita completa literatura no patente (LNP)					
Apellido, A. A (Fecha). Título del artículo. Nombre de la revista. Volumen(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: (27/04/2026)					

