

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 9590 de 17 de junio de 2025

Ref. Expediente N° NC2022/0000054

Señores

Luis Eduardo GUTIERREZ SHERIS

TÍTULO DE LA SOLICITUD: “SISTEMA Y MÉTODO MEDIANTE EL USO DE UN CONSENSO DE GRADIENTE DE IDONEIDAD DE LA CADENA DE BLOQUES”

NUMERO DE SOLICITUD INTERNACIONAL: PCT/US2020/037795.

FECHA DE PRESENTACIÓN INTERNACIONAL: 15 de junio de 2020.

PRIORIDAD: 13/06/2019, US (ESTADOS UNIDOS DE AMÉRICA), 62/861,086.

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 4 de abril de 2025 bajo el número NC2022/0000054, 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 proporcionar un sistema y método informático para la implementación de un libro mayor electrónico distribuido o cadena de bloques que usa un método de consenso de Gradiente de Idoneidad para determinar cuál de los nodos que compiten se selecciona para recibir una recompensa por un bloque particular o una cadena que se ha agregado a la cadena de bloques.

Para resolver dicho problema técnico, la solicitud en estudio plantea un método de consenso de la cadena de bloques de Gradiente de Idoneidad, donde el consenso de Gradiente de Idoneidad se implementa dentro de un sistema de la cadena de bloques y una red que consiste de los Nodos de Construcción de Bloques. Cuando un nuevo Nodo de Construcción de Bloques se conecta en línea, se conecta a la red al emparejarse con otros Nodos de Construcción de Bloques ya conectados a la red. Un Nodo de Construcción de Bloques recientemente conectado descarga los bloques de la cadena de bloques, encabezados de bloques, contratos inteligentes, registros de datos y transacciones de nodos pares dentro de la red de nodo.

3. Reivindicaciones estudiadas

El presente estudio se basa en el capítulo reivindicatorio presentado el 4 de abril de 2025.

4. Determinación del Estado de la Técnica

La fecha para determinar el estado de la técnica es el 13 de junio de 2019, que corresponde a la fecha de presentación de prioridad de la solicitud.

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	US2017/0075941	"Consensus system and method for adding data to a blockchain"	16 de marzo de 2017
D3	Kokoris-Kogias, E., Jovanovic, P., Gasser, L., Gailly, N., Syta, E., & Ford, B.	"OmniLedger: A Secure, Scale-Out, Decentralized Ledger via Sharding"	26 de julio de 2018

D1¹ divulga un método y un aparato para alcanzar un consenso sobre la adición de datos a un sistema de registro distribuido sin autoridad central de confianza. Este método comprende el envío de un mensaje de anuncio desde un dispositivo conectado a una pluralidad de dispositivos conectados a través de una red peer-to-peer. Dicho mensaje proporciona la identificación del dispositivo mediante una clave pública (un par de claves pública/privada), un identificador de dirección único y un hash. Posteriormente, tras un periodo de espera medido, por ejemplo, en tiempo o bloques de datos, el dispositivo conectado puede enviar los datos para su inclusión en el registro distribuido. Si el mensaje de anuncio y los datos anteriores en el registro distribuido cumplen una condición predeterminada, la pluralidad de dispositivos conectados pueden incluir los datos en el registro distribuido. Si el dispositivo conectado no envía los datos cuando se cumple la condición predeterminada, el mensaje de anuncio puede cancelarse (Resumen).

D3² divulga un novedoso libro mayor distribuido y escalable que preserva la seguridad a largo plazo en operaciones sin permisos. Garantiza la seguridad y la corrección mediante un protocolo de aleatoriedad pública resistente a sesgos para seleccionar fragmentos grandes y estadísticamente representativos que procesan transacciones, e introduce un protocolo eficiente de confirmación entre fragmentos que gestiona de forma atómica las transacciones que afectan a múltiples fragmentos. OmniLedger también optimiza el rendimiento mediante el procesamiento paralelo de transacciones dentro de los fragmentos, la poda del libro mayor mediante bloques de estado firmados colectivamente y la validación de baja latencia "confiar pero verificar" para transacciones de bajo valor. Una evaluación de nuestro prototipo experimental muestra que el rendimiento de OmniLedger escala linealmente en función del número de validadores activos, lo que permite soportar cargas de trabajo de nivel Visa y superiores, a la vez que confirma transacciones típicas en menos de dos segundos (Resumen).

5. 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.

5.1. Nivel Inventivo

Teniendo en cuenta lo señalado en el artículo 18 de la Decisión 486 de 2000 de la Comisión de la Comunidad Andina, la reivindicación independiente 1 (NC2022/0000054 del 4 de abril de 2025) refiere a: *“Un método implementado por computador en una red*

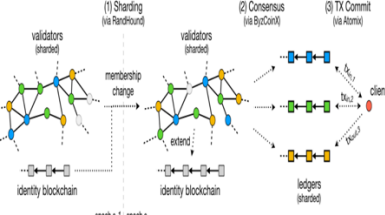
¹ <https://patentimages.storage.googleapis.com/79/79/dc/ed9f656e0f1a58/US20170075941A1.pdf>
² Kokoris-Kogias, E., Jovanovic, P., Gasser, L., Gailly, N., Syta, E., & Ford, B. (2018, May). Omniledger: A secure, scale-out, decentralized ledger via sharding. In 2018 IEEE symposium on security and privacy (SP) (pp. 583-598). IEEE. Recuperado desde: <https://eprint.iacr.org/2017/406.pdf>

Oficio N° 9590 de 17 de junio de 2025

Ref. Expediente N° NC2022/0000054

informática, comprendiendo el método implementado por computador: (...)”. A continuación, se presenta la tabla comparativa entre el objeto reivindicado y los documentos encontrados en el estado de la técnica:

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

CARACTERÍSTICAS ESENCIALES	D1	D3
Un método implementado por computador en una red informática, comprendiendo el método implementado por computador:	Sistema de consenso y método para agregar datos a una cadena de bloques (Título).	(...) OmniLedger permite a los validadores cambiar de forma segura y eficiente entre fragmentos, sin estar limitados a un único método de ataque anti-Sybil y sin demoras entre eventos de reconfiguración (...) (Pág 13. Col. Der, Sec. XI).
Configurar un libro mayor electrónico distribuido en la memoria electrónica (114) de una o más computadoras (110) en un sistema de cadenas de bloques (100).	(...) métodos relacionados con la adición de datos a un libro de contabilidad distribuido o cadena de bloques (...) (Párr. 0001).	No menciona.
El libro mayor electrónico distribuido tiene una pluralidad de bloques interconectados hacia atrás (200), dispuestos como una o más instancias de estructuras de datos de cadena de bloques lineales, arreglos de bloques no lineales, mallas n-dimensionales o estructuras de datos reticulares, o gráficos acíclicos dirigidos.	(...) Los datos contenidos dentro del bloque de contabilidad (612) pueden contener un valor hash equivalente (634) de valor igual a un valor hash del bloque anterior, siendo el hash con la etiqueta (624) el que vincula el bloque de contabilidad (612) al bloque de contabilidad (610) (...) (Párr. 0091). No menciona que la conexión sea hacia atrás.	(...) Los registros distribuidos derivan el estado actual del sistema a partir de una cadena de bloques, o una secuencia de bloques totalmente ordenados que contienen transacciones (...) (Pág. 2, Col. Der, Sec. B). En la siguiente figura se muestran las conexiones hacia atrás.  Pág. 4, fig. 2
Configurar cada uno de los bloques interconectados (210A, 210B, 210C) para incluir un conjunto ordenado de registros de datos individuales (220A-C), de modo que al menos uno de los registros refleje una transformación de al menos una parte del estado global del libro mayor electrónico distribuido.	(...) La pluralidad de dispositivos conectados a la red puede determinar un candidato secundario, un candidato terciario, etc., aplicando el mismo criterio para ordenar el conjunto de diferencias con el fin de construir una lista de candidatos (Párr. 0033). La FIG. 5 ilustra cómo la pluralidad de dispositivos conectados a la red que comprenden un conjunto de nodos validadores puede determinar si el dispositivo conectado a la red que envía el mensaje de anuncio de minero puede contribuir a la adición de un bloque de datos al libro mayor distribuido en un momento dado o en un estado	(...) Los registros distribuidos derivan el estado actual del sistema a partir de una cadena de bloques, o una secuencia de bloques totalmente ordenados que contienen transacciones (...) (Pág. 2, Col. Der, Sec. B).



Oficio N° 9590 de 17 de junio de 2025

Ref. Expediente N° NC2022/0000054

	dado del libro mayor distribuido (Párr. 0072).	
Configurar el sistema de cadenas de bloques (100) para que comprenda una red peer-to-peer de nodos de computador, con una o más computadoras configuradas como nodos billetera (120), y con una o más computadoras configuradas como nodos de construcción de bloques (110).	(...) uno o más procesadores y medios de almacenamiento que comprenden instrucciones de computadora, dicha pluralidad de dispositivos conectados a la red se pueden conectar entre sí a través de una red peer-to-peer, dispuestos de tal manera que cuando se ejecutan instrucciones de computadora en uno o más procesadores de uno o más de la pluralidad de dispositivos conectados a la red, se provocan operaciones para alcanzar un consenso para agregar un bloque de datos a un libro mayor distribuido (...) (Reiv. 10).	No menciona.
Configurar el uno o más nodos de billetera (120) para transmitir uno o más de los registros de datos a uno o más nodos de construcción de bloques (110) en la red peer-to-peer.	La FIG. 7 es un diagrama que ilustra cómo actúan la red peer to peer y los nodos validadores cuando un candidato principal para enviar un bloque no lo hace, un candidato secundario envía el bloque en su lugar y se produce una revocación del mensaje de anuncio del minero del candidato principal que no envía el siguiente bloque de datos dentro de un tiempo apropiado (Párr. 0044). (...) El bloque de datos también puede contener otros mensajes y elementos, por ejemplo, pero no limitado a, otros mensajes de anuncios de mineros, datos de transacciones financieras, anuncios de claves y/o revocación de claves (...) (Párr. 0069). En el estado de la técnica resulta evidente que los procesamiento de pago pueden asociarse a una billetera.	(...) Presentamos OmniLedger, la primera arquitectura DL que ofrece una capacidad de procesamiento de transacciones escalable, competitiva con los sistemas centralizados de procesamiento de pagos, como Visa. (...) (Pág. 1, Col. Izq. Sec. I Párr. 3). En el estado de la técnica resulta evidente que los procesamiento de pago pueden asociarse a una billetera.
Configurar el uno o más nodos de construcción de bloques (110) para construir uno o más bloques interconectados (210A, 210B, 210C) en el libro mayor electrónico distribuido seleccionando y ordenando uno o más de los registros de datos para incluirlos en dicho uno o más nuevos bloques interconectados.	Un bloque de contabilidad posterior (616) puede contener un mensaje de anuncio de minero (517) para el nodo validador (107), con un Número de Identificación de Minero (502), o MIN, que comienza con los dígitos hexadecimales 9E6C. El bloque de contabilidad posterior (616) puede vincularse con el bloque de contabilidad posterior (614) que lo precede mediante la inclusión de un valor (638) en el bloque de contabilidad posterior (616) con	(...) Durante el arranque, los nuevos nodos (completos) rastrean todo el libro mayor distribuido y crean una base de datos de UTXO válidos, necesaria para decidir posteriormente si se puede aceptar un nuevo bloque. El modelo UTXO fue introducido por Bitcoin, pero ha sido ampliamente adoptado por otros sistemas de libro mayor distribuido (Pág. 2, Col. Der, Sec. B)..



Oficio N° 9590 de 17 de junio de 2025

Ref. Expediente N° NC2022/0000054

	un valor equivalente al hash de los datos (628) encapsulados en el bloque de contabilidad posterior (614), ampliando así la lista enlazada (Párr. 0094). La FIG. 6 es un diagrama que muestra la participación de tres dispositivos conectados a la red que actúan como mineros, o nodos validadores, para determinar el siguiente bloque de datos que se puede agregar al libro mayor distribuido, de acuerdo con una realización de la presente invención (Párr. 0043).	
E implementar en el sistema de cadenas de bloques (100), un proceso de propagación de datos de confiar, pero verificar, en donde al menos un nodo de construcción de bloques (110) está configurado para crear al menos un nuevo bloque interconectado en el sistema de cadenas de bloques (100) antes de verificar la corrección de uno o más bloques precedentes a los que dicho al menos un nuevo bloque interconectado se vincula.	No menciona el proceso confiar, pero verificar. El nodo validador (107) puede entonces proceder a construir un nuevo bloque de datos (622), que comprende un valor de enlace de retroceso (642) igual al hash ejemplar (640), una copia del MIN (646), y un hash de un dato que comprende el nuevo bloque de datos (644) (Párr. 0097).	OmniLedger admite la validación opcional de confianza pero verificación, en la que un primer nivel pequeño de validadores procesa las transacciones rápidamente y luego las transfiere a un segundo nivel más grande, y por lo tanto más lento, que vuelve a verificar la corrección de las transacciones del primer nivel y garantiza la seguridad a largo plazo (...) (Pág. 4, Col. Izq. Párr. 3). (...) La implementación de OmniLedger con validación de dos niveles, "confiar pero verificar", proporciona un rendimiento de 2250 tps con una latencia de primer nivel de cuatro segundos ante un adversario del 25 % (...) (Pág. 4, Col. Izq. Párr. 4).

D1 es considerado como el estado de la técnica más cercano a la invención definida en la reivindicación 1, ya que divulga un sistema de consenso y método para agregar datos a una cadena de bloques (Título).

La diferencia entre la invención definida entre la reivindicación 1 y el método divulgado en D1, consiste en que la solicitud incluye el proceso confiar, pero verificar y una pluralidad de bloques interconectados hacia atrás.

El efecto que se logra al incluir el proceso confiar, pero verificar y una pluralidad de bloques interconectados hacia atrás es aumentar el rendimiento transaccional de la cadena de bloques.

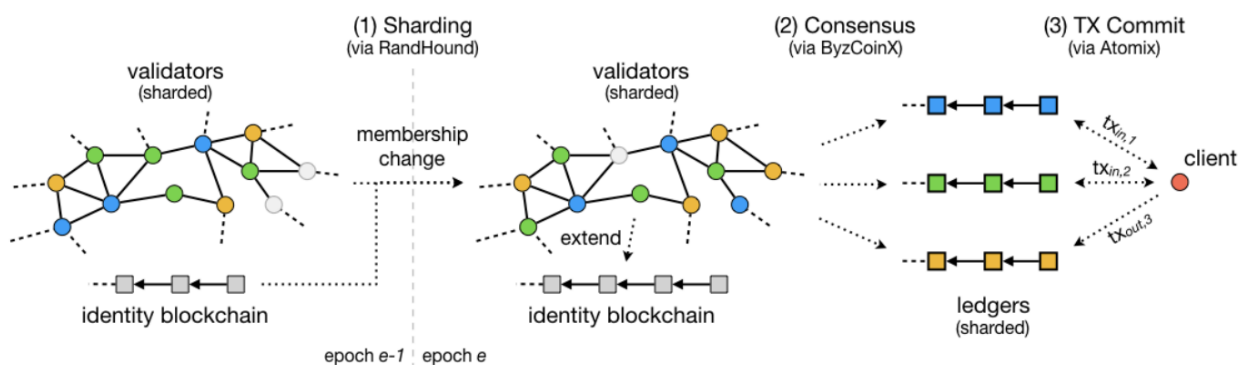
Por lo tanto, el problema técnico objetivo que pretende resolver esta invención se puede formular así: ¿cómo modificar el método divulgado en D1 para aumentar el rendimiento transaccional de la cadena de bloques?

Sin embargo, el incluir el proceso confiar, pero verificar y una pluralidad de bloques interconectados hacia atrás para aumentar el rendimiento transaccional de la cadena de

Oficio N° 9590 de 17 de junio de 2025

Ref. Expediente N° NC2022/0000054

bloques, ya está divulgado en D3 que se refiere a (...) OmniLedger admite la validación opcional de confianza pero verificación, en la que un primer nivel pequeño de validadores procesa las transacciones rápidamente y luego las transfiere a un segundo nivel más grande, y por lo tanto más lento, que vuelve a verificar la corrección de las transacciones del primer nivel y garantiza la seguridad a largo plazo (...) (Pág. 4, Col. Izq. Párr. 3). (...) La implementación de OmniLedger con validación de dos niveles, "confiar pero verificar", proporciona un rendimiento de 2250 tps con una latencia de primer nivel de cuatro segundos ante un adversario del 25 % (...) (Pág. 4, Col. Izq. Párr. 4). (...) Los registros distribuidos derivan el estado actual del sistema a partir de una cadena de bloques, o una secuencia de bloques totalmente ordenados que contienen transacciones (...) (Pág. 2, Col. Der, Sec. B). En la siguiente figura se muestran las conexiones hacia atrás.



Pág. 4, fig. 2

En consecuencia, la persona normalmente versada en la materia al verse enfrentada al problema técnico objetivo de aumentar el rendimiento transaccional de la cadena de bloques estaría motivada a incluir proceso confiar, pero verificar y una pluralidad de bloques interconectados hacia atrás del D3 en el método de D1, para así llegar al objeto de la reivindicación 1. Por lo cual se considera obvia.

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

- Reivindicación 3: El nodo validador (107) puede entonces proceder a construir un nuevo bloque de datos (622), que comprende un valor de enlace de retroceso (642) igual al hash ejemplar (640), una copia del MIN (646), y un hash de un dato que comprende el nuevo bloque de datos (644) (Párr. 0097).

- Reivindicación 4: Como se muestra, la red peer-to-peer 108 está incorporada dentro de una red de conmutación de paquetes 101, a través de la interconexión de la pluralidad de dispositivos conectados a la red en la red peer-to-peer 108 (Párr. 0046).

- Reivindicación 5: El nodo validador (106) puede entonces transmitir el bloque de datos que contiene el mensaje de anuncio del minero a la red peer-to-peer según el paso (418) (Párr. 0070). Mediante la transmisión a la red peer-to-peer, el bloque de datos puede llegar a otro dispositivo conectado a la red (107), que puede ser otro nodo validador o un nodo estándar. El otro dispositivo conectado a la red (107) puede entonces repetir el mismo cálculo realizado previamente por el nodo validador (106) en el paso (410), y el cálculo puede devolver un resultado exitoso o un error (420). Si el resultado es un error, el otro dispositivo conectado a la red (107) puede determinar que el nodo validador (106) no es un candidato adecuado y puede descartar el bloque, como se muestra en el paso (422). Si el cálculo produce un resultado exitoso, el otro dispositivo conectado a la red

Oficio N° 9590 de 17 de junio de 2025

Ref. Expediente N° NC2022/0000054

107 puede determinar que el nodo validador (106) es un candidato adecuado y puede añadir el bloque de datos a una copia del libro mayor distribuido (424) (Párr. 0071).

- Reivindicación 16: Mediante la transmisión a la red peer-to-peer, el bloque de datos puede llegar a otro dispositivo conectado a la red (107), que puede ser otro nodo validador o un nodo estándar. El otro dispositivo conectado a la red (107) puede repetir el mismo cálculo realizado previamente por el nodo validador (106) en el paso (410), y el cálculo puede arrojar un resultado correcto o un error (420). Si el resultado es correcto, el otro dispositivo conectado a la red (107) puede determinar que el nodo validador (106) no es un candidato adecuado y descartar el bloque, como se muestra en el paso (422). Si el cálculo es correcto, el otro dispositivo conectado a la red (107) puede determinar que el nodo validador (106) es un candidato adecuado y añadir el bloque de datos a una copia del libro mayor distribuido 424 (Párr. 0071). En otras realizaciones de la invención, cada bloque puede estar vinculado al bloque anterior mediante la inclusión de una raíz hash de uno o más de, pero no limitado a: un árbol de Merkle, un árbol de Patricia, un árbol de radix o alguna otra función que tome como entrada uno o más de los bloques anteriores (Párr. 0093).

- Reivindicación 17: (...) método y un aparato para alcanzar un consenso sobre la adición de datos a un sistema de registro distribuido sin autoridad central de confianza. Este método comprende el envío de un mensaje de anuncio desde un dispositivo conectado a una pluralidad de dispositivos conectados a través de una red peer-to-peer. Dicho mensaje proporciona la identificación del dispositivo mediante una clave pública (un par de claves pública/privada), un identificador de dirección único y un hash. Posteriormente, tras un periodo de espera medido, por ejemplo, en tiempo o bloques de datos, el dispositivo conectado puede enviar los datos para su inclusión en el registro distribuido. Si el mensaje de anuncio y los datos anteriores en el registro distribuido cumplen una condición predeterminada, la pluralidad de dispositivos conectados pueden incluir los datos en el registro distribuido. Si el dispositivo conectado no envía los datos cuando se cumple la condición predeterminada, el mensaje de anuncio puede cancelarse (Resumen).

- Reivindicación 18: Otro sistema de consenso, denominado "tolerancia práctica a fallos bizantinos", se implementa mediante múltiples rondas de votación entre los participantes, lo que requiere que los mensajes en la red se firmen varias veces. Esto genera una sobrecarga computacional para calcular las firmas y una sobrecarga de espacio en disco para almacenar todas las firmas generadas (Párr. 0010). (...) el mensaje de anuncio puede estar firmado por el primero de la pluralidad de dispositivos conectados a la red utilizando una clave privada del par de claves pública/privada (Párr. 0027). Las operaciones comienzan cuando el primero de la pluralidad de dispositivos conectados a la red genera un mensaje de anuncio que puede indicar la intención del primero de la pluralidad de dispositivos conectados a la red de convertirse en un minero de la cadena de bloques o el libro mayor distribuido, que comprende una clave pública de un par de claves pública/privada, un identificador de dirección único y un hash de la clave pública y el identificador de dirección único (Párr. 0018). Puede estar presente un almacenamiento adicional (212), que puede contener una partición o componente criptográficamente seguro (214), donde se pueden almacenar de forma segura claves criptográficas (Párr. 0052).

De igual manera, D3 divulga las características de las reivindicaciones dependientes así:

- Reivindicación 2: (...) una prueba Merkle firmada contra el bloque donde se incluye la transacción (Col. 6, Col. Izq. Numeral 2). (...) OmniLedger admite la validación opcional de confianza pero verificación, en la que un primer nivel pequeño de validadores procesa

Oficio N° 9590 de 17 de junio de 2025

Ref. Expediente N° NC2022/0000054

las transacciones rápidamente y luego las transfiere a un segundo nivel más grande (Pág. 4, Col. Izq. Párr. 3). (...) La implementación de OmniLedger con validación de dos niveles, "confiar pero verificar", proporciona un rendimiento de 2250 tps con una latencia de primer nivel de cuatro segundos ante un adversario del 25 % (...) (Pág. 4, Col. Izq. Párr. 4). (...) Los registros distribuidos derivan el estado actual del sistema a partir de una cadena de bloques, o una secuencia de bloques totalmente ordenados que contienen transacciones (...) (Pág. 2, Col. Der, Sec. B).

- Reivindicación 3: (...) permitimos que los validadores soliciten la confirmación de transacciones, ya que consideran que están censuradas. Pueden recopilar dichas transacciones mediante el proceso habitual de intercambio de información o recibir una solicitud directamente de un cliente. Este protocolo puede ejecutarse periódicamente (por ejemplo, una vez cada 10 bloques). Denotamos que existen $N = 3f + 1$ validadores, donde como máximo f son deshonestos (Pág. 14, Col. Der, Sec. Apendice A, Párr. 2).

- Reivindicación 4: (...) permitimos que los validadores soliciten la confirmación de transacciones, ya que consideran que están censuradas. Pueden recopilar dichas transacciones mediante el proceso habitual de intercambio de información o recibir una solicitud directamente de un cliente. Este protocolo puede ejecutarse periódicamente (por ejemplo, una vez cada 10 bloques). Denotamos que existen $N = 3f + 1$ validadores, donde como máximo f son deshonestos (Pág. 14, Col. Der, Sec. Apendice A, Párr. 2).

- Reivindicación 10: (...) Para capturar el procesamiento concurrente de bloques, adoptamos un gráfico acíclico dirigido basado en bloques (blockDAG) [33] como estructura de datos, donde cada bloque puede tener varios padres (...) (Pág. 7, Col. Der. Sec. B Párr. 3).

- Reivindicación 11: (...) Para capturar el procesamiento concurrente de bloques, adoptamos un gráfico acíclico dirigido basado en bloques (blockDAG) (...) (Pág. 7, Col. Der. Sec. B Párr. 3). (...) una prueba Merkle firmada contra el bloque donde se incluye la transacción (Col. 6, Col. Izq. Numeral 2). (...) OmniLedger admite la validación opcional de confianza pero verificación, (...) (Pág. 4, Col. Izq. Párr. 3). (...) La implementación de OmniLedger con validación de dos niveles, "confiar pero verificar", proporciona un rendimiento de 2250 tps con una latencia de primer nivel de cuatro segundos ante un adversario del 25 % (...) (Pág. 4, Col. Izq. Párr. 4).

- Reivindicación 12: (...) El límite de sincronía Δ garantiza que el ticket de un líder honesto sea visto por todos los demás validadores honestos. Si el adversario gana la lotería, puede decidir entre cumplir y ejecutar el protocolo RandHound o fallar, lo que excluye a ese nodo de participar por el resto de la época (...) (Pág. 5, Col. Izq. Párr. 3).

- Reivindicación 13: (...) cuando los validadores principales detectan una inconsistencia, la respectiva transacción validada optimistamente se excluye y los validadores que firmaron el bloque inválido se identifican y se les exige responsabilidad, por ejemplo, reteniendo cualquier recompensa o excluyéndolos del sistema (...) (Pág. 8, Col. Der. Párr. 3).

- Reivindicación 15: Los libros de contabilidad distribuidos derivan el estado actual del sistema a partir de una cadena de bloques, o una secuencia de bloques totalmente ordenados que contienen transacciones. OmniLedger adopta el modelo de salida de transacción no gastada (UTXO) para representar el estado del libro de contabilidad, debido a su simplicidad y paralelización. En este modelo, las salidas de una transacción crean nuevas UTXO (y les asignan créditos), y las entradas "gastan" completamente las UTXO existentes. Durante el arranque, los nuevos nodos (completos) rastrean todo el



Oficio N° 9590 de 17 de junio de 2025

Ref. Expediente N° NC2022/0000054

libro de contabilidad distribuido y crean una base de datos de UTXO válidas, necesaria para decidir posteriormente si se puede aceptar un nuevo bloque. El modelo UTXO fue introducido por Bitcoin, pero ha sido ampliamente adoptado por otros sistemas de libros de contabilidad distribuidos (Pág. 2, Col. Der. Sec. B).

- Reivindicación 17: Muchos enfoques presentan diferentes compensaciones en términos de seguridad y rendimiento. Reemplazar el consenso de Nakamoto con PBFT, por ejemplo, puede aumentar el rendimiento y, al mismo tiempo, reducir la latencia de confirmación de transacciones (Pág. 1, Col. Izq. Sec. I, Párr. 1).

- Reivindicación 19: (...) cuando los validadores principales detectan una inconsistencia, la respectiva transacción validada optimistamente se excluye y los validadores que firmaron el bloque inválido se identifican y se les exigen responsabilidades, por ejemplo, reteniendo cualquier recompensa o excluyéndolos del sistema. Cabe destacar que los detalles exactos de dichas sanciones dependen del esquema de incentivos, que queda fuera del alcance de este documento. Dado un incentivo mínimo para el mal comportamiento y la confianza cuantificable en la seguridad de la validación optimista (Figura 5), los clientes pueden optar, según sus necesidades, por aprovechar el procesamiento en tiempo real con una garantía optimista de finalización o por esperar a que su transacción se finalice (Pág. 8, Col. Der, Párr. 3 a Pág. 9 Col. Izq, Párr. 1).

Las reivindicaciones dependientes 2 a 20 tampoco cumplen con el requisito de nivel inventivo.

6. Conclusión

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

Ítem	Documento	Reivindicaciones afectadas	Requisito que afecta
D1	US2017/0075941	1 a 20	Nivel inventivo
D3	Kokoris-Kogias, E., Jovanovic, P., Gasser, L., Gailly, N., Syta, E., & Ford, B.	1 a 20	Nivel inventivo

7. Respuesta a los argumentos del solicitante

Argumentos con respecto a la claridad

El solicitante indica que “Con respecto a la redacción de “interconectados retroconectados” y “computadors” en la reivindicación 1, me permito señalar que se ha reemplazado la expresión “retroconectados” por la expresión “hacia atrás” de acuerdo con lo divulgado en la descripción. De igual manera se reemplazó el término “computadors” por “computadoras” y corregir el error tipográfico. Por lo tanto, se superan dichas objeciones.

En cuanto al término “protocolo de chismes”, me permito señalar que ha sido reemplazado por la expresión “protocolo gossip” de acuerdo con lo divulgado en la descripción y así superar el error de traducción. Por lo cual, se solicita el retiro de dicha objeción.

Considerando las sugerencias del Examinador y el hecho que la materia reclamada en el Capítulo Reivindicatorio adjunto al presente memorial cumple con las disposiciones del Artículo 30 de la Decisión 486, y corresponden a una limitación razonable del concepto



Oficio N° 9590 de 17 de junio de 2025

Ref. Expediente N° NC2022/0000054

inventivo desarrollado por el inventor, de manera atenta solicito a ese Despacho retirar las objeciones en cuanto a la claridad de la materia reclamada”.

Con respecto a lo anterior, es importante indicar que las objeciones de claridad han sido superadas y el nuevo capítulo reivindicatorio se presenta de manera que cumple con lo estipulado en el artículo 30 de la decisión 486.

Argumentos con respecto al nivel inventivo

El solicitante indica que *“Sin embargo, **D1** no divulga o sugiere un esquema de confiar, pero verificar y tampoco proporciona alguna enseñanza relacionada con dichos esquemas ni con que el libro mayor electrónico distribuido tiene una pluralidad de bloques interconectados hacia atrás, dispuestos como una o más instancias de estructuras de datos de cadena de bloques lineales, arreglos de bloques no lineales, mallas n-dimensionales o estructuras de datos reticulares, o gráficos acíclicos dirigidos, tal como se requiere en la reivindicación 1 actualmente reclamada. Por lo tanto, la presente solicitud es inventiva con respecto a las enseñanzas de **D1**”.*

Con respecto a lo anterior, es importante aclarar que, el requisito que la solicitud no logra superar es el de nivel inventivo, por lo tanto, el análisis debe realizarse con respecto a lo sugerido por el estado de la técnica junto al conocimiento del técnico medio versado en la materia. Para el caso específico, D1 no sugiere el protocolo “confiar, pero verificar”, sin embargo, el documento D3 en la página 4, columna izquierda párrafos 3 y 4 incluye la característica en la cual se implementa el protocolo confiar, pero verificar. Adicionalmente, es importante resaltar que tanto D1 como D3 son documentos relacionados con el estado de la técnica, por lo tanto, para el técnico resulta evidente combinar las anterioridades para llegar al objeto planteado en la solicitud. Teniendo en cuenta las anteriores consideraciones, el argumento no es procedente y se trasladan nuevas objeciones de nivel inventivo.

El solicitante indica que *“Por otro lado, y con el fin de “curar” las deficiencias de **D1**, el examinador cita el documento **D2** porque describe un sistema mejorado para procesar transacciones con una moneda criptográfica. También enseña que el sistema utiliza un protocolo de cadena de bloques como registro público de transacciones para garantizar que solo se puedan usar tokens válidos como entrada de transacción y que solo se puedan usar una vez. Los testigos integran las transacciones en una cadena de bloques y una vez que suficientes testigos confirman un bloque, este se convierte en una parte permanente e indeleble de la cadena de bloques, y por lo cual, un experto en la materia podría llegar a la materia reivindicada en la presente solicitud de forma obvia. Sin embargo, **D2** no divulga o sugiere un esquema de confiar, pero verificar y tampoco proporciona alguna enseñanza relacionada con dichos esquemas ni con que el libro mayor electrónico distribuido tiene una pluralidad de bloques interconectados hacia atrás, dispuestos como una o más instancias de estructuras de datos de cadena de bloques lineales, arreglos de bloques no lineales, mallas n-dimensionales o estructuras de datos reticulares, o gráficos acíclicos dirigidos, tal como se requiere en la reivindicación 1 actualmente reclamada. Por lo cual, es evidente que las enseñanzas de **D1** y **D2** solos o en combinación no habrían motivado a un experto en la materia para llegar de forma obvia a la invención tal como se reivindica actualmente. Por tanto, se evidencia una actividad inventiva de la presente solicitud en vista del arte previo citado **D1** y **D2**.”*

Con respecto a lo anterior, es importante indicar que en el argumento anterior se respondió como es realizada la afectación del protocolo “confiar, pero verificar”. Adicionalmente, vale la pena aclarar que, los argumentos relacionados con el documento D2 son procedentes toda vez que no logran sugerir las características técnicas

Oficio N° 9590 de 17 de junio de 2025

Ref. Expediente N° NC2022/0000054

reclamadas por el señor solicitante. Si embargo, esta Oficina realiza una nueva búsqueda en la cual se encuentra el documento D3 que, junto a D1 afectan el nivel inventivo de la solicitud.

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
DIRECTORA DE NUEVAS CREACIONES

Oficio N° 9590 de 17 de junio de 2025

Ref. Expediente N° NC2022/0000054

INFORME DE BÚSQUEDA
EXAMEN DE PATENTABILIDAD

Solicitud No.		Examen de patentabilidad							
NC2022/0000054		1°	-	2°	X	3°	-	Revoca	-
Solicitud Internacional No.		Fecha solicitud internacional: (DD/MM/AÑO)							
PCT/US2020/037795		15 de junio de 2020							
Fecha de determinación estado de la técnica (DD/MM/AÑO)				Prioridad		Presentación			
13/06/2019				X		-			
Solicitante									
Luis Eduardo GUTIERREZ SHERIS									
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 20					
Palabras clave utilizadas				Blockchain, ledger, linear, non-linear, bloom, Nakamoto, graph, signature, tree, merkle, "trust-but-verify", protocol, node, Nakamoto, consensus, blockchain.					
Clasificaciones utilizadas para la búsqueda				CIP:	G06F 15/173				
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	NC2018/0004808	19/07/2018	-	-			A		
WO	US2017075941	16/07/2017	1 a 20	Todo el documento			Y		
	WO2018189657	18/10/2018	-	-					
	CN108960837	07/12/2018	-	-					
	US2018373776	27/12/2018	-	-					
EPO	Kokoris-Kogias, E., Jovanovic, P., Gasser, L., Gailly, N., Syta, E., & Ford, B.	26/07/2018	1 a 20	Todo el documento			Y		
Patbase	US2018091524	29/03/2018	-	-			A		
Orbit	US11456874	27/09/2022	-	-			T		
⁽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.		Kokoris-Kogias, E., Jovanovic, P., Gasser, L., Gailly, N., Syta, E., & Ford, B. (2018, May). Omniledger: A secure, scale-out, decentralized ledger via sharding. In 2018 IEEE symposium on security and privacy (SP) (pp. 583-598). IEEE. Recuperado desde: https://eprint.iacr.org/2017/406.pdf							
⁽²⁾ Categorías de documentos citados									
"A" Documento que define el estado general de la técnica no considerado como particularmente relevante.					"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				
"E" Solicitud de patente o patente anterior pero publicada en la fecha de presentación internacional o en fecha posterior.									



Oficio N° 9590 de 17 de junio de 2025

Ref. Expediente N° NC2022/0000054

“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.	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: (11/06/2025)	