

Señor

**DIRECTOR DIVISIÓN DE NUEVAS CREACIONES
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**

E. S. D.

REF: Expediente No. **NC2022/0000054**, solicitud de patente de invención a favor de **Luis Eduardo GUTIERREZ-SHERIS**, Título: **SISTEMA Y MÉTODO MEDIANTE EL USO DE UN CONSENSO DE GRADIENTE DE IDONEIDAD DE LA CADENA DE BLOQUES**

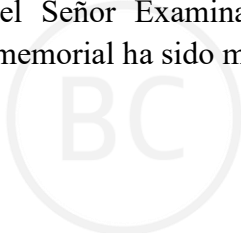
RESPUESTA A EXAMEN DE FONDO

JUAN PABLO CADENA SARMIENTO, portador de la tarjeta profesional No. 57.492 del C.S.J., obrando como apoderado de la sociedad solicitante me permito dar respuesta al Oficio No. 9590 relacionado con la patentabilidad de la presente invención y notificado el 18 de junio de 2025.

En respuesta a las observaciones realizadas como resultado del examen de fondo, es pertinente mencionar que las reivindicaciones cumplen a cabalidad con los requerimientos de patentabilidad establecidos en la Decisión 486 de 2000, razón por la que respetuosamente disiento de los comentarios del Examinador a este respecto. A continuación, sin embargo, se presentan argumentos y se mencionan las modificaciones realizadas para atender a cada uno de los requerimientos del Examinador:

1. Modificación a las reivindicaciones

Me permito dirigir la atención del Señor Examinador en el hecho que el Capítulo Reivindicatorio adjunto al presente memorial ha sido modificado de la siguiente manera:



- Se ha modificado la reivindicación 1 eliminando la expresión *“a los que dicho al menos un nuevo bloque interconectado se vincula”*, con el fin de dar claridad a la materia a proteger.
- Se ha reemplazado la expresión *“un protocolo gossip”* por la expresión *“una red de intercambio de datos”* en la reivindicación 2, para dar mayor claridad a la presente invención.
- Se ha modificado la reivindicación 3 eliminando las expresiones *“el protocolo gossip permite que”* y *“a través del protocolo gossip”*, para dar mayor claridad a la presente invención.
- Se ha modificado la reivindicación 4 eliminando la expresión *“el protocolo gossip permite transmitir”* y se ha reescrito dicha reivindicación incluyendo la característica *“se propaga a través del sistema de cadenas de bloques, que además incluye (...)”*, con el fin de dar mayor claridad a la presente invención.
- Se ha modificado la reivindicación 14 para especificar que además se incluye *“una etapa de comparar”*, con el fin de dar mayor claridad a la presente invención.
- Se incluyeron las nuevas reivindicaciones 17 y 18 que recitan:

“17. El método implementado por computador de las reivindicaciones 1 a 16, en donde el sistema de cadena de bloques (110) impone un retraso de tiempo entre el al menos un nuevo bloque interconectado y al menos un bloque interconectado subsecuente al requerir un espacio mínimo de tiempo entre bloques” y

“18. El método implementado por computador de la reivindicación 17, en donde el espacio mínimo de tiempo entre bloques es un segmento de tiempo cuantificado por un número mínimo de unidades informáticas para ejecutarse en secuencia”

En consecuencia, la numeración y dependencia de las reivindicaciones ha sido modificada de conformidad con lo anteriormente mencionado.

Así las cosas, es importante mencionar que las modificaciones realizadas a las reivindicaciones cumplen en su totalidad con los requisitos establecidos en el Artículo 34 de la Decisión 486, teniendo en cuenta que estas **no involucran una ampliación a la protección**

correspondiente a la divulgación tal y como se presentó originalmente. Por el contrario, el Capítulo Reivindicatorio Modificado y adjunto al presente memorial cumple con los lineamientos establecidos por la Decisión Andina 486 y encuentra sustento a lo largo de la memoria descriptiva de la solicitud.

2. Nivel Inventivo

Con respecto al nivel inventivo de la presente solicitud, el Examinador asegura que las reivindicaciones **1 a 20** carecen de nivel inventivo en vista de las enseñanzas de los documentos **D1** y **D3**.

En respuesta a lo anterior, de manera atenta me permito manifestar que contrario a los señalamientos establecidos por el Examinador, la presente solicitud, tal y como se encuentra reclamada en el Capítulo Reivindicatorio adjunto a este memorial goza de nivel inventivo y presenta diferencias con los documentos del arte previo citados en el Oficio Técnico No. 9590.

En primer lugar, me permito aclarar que el Capítulo Reivindicatorio ha sido modificado y limitado a elementos específicos que permiten definir la materia reivindicada en la presente solicitud haciendo que difiera completamente de las enseñanzas de **D1** y **D3**.

Además, me permito señalar que el campo al que se refiere la invención reclamada se encuentra dentro de la técnica de *blockchain* (cadena de bloques); particularmente en lo relacionado con métodos de consenso de *Gradiente de Idoneidad*. En este sentido, y considerando que este tipo de métodos tienen como objetivo que cualquier intercambio de información (por ejemplo una *transacción de información*) realizada mediante *blockchain* debe ser validada para cumplir y/o incrementar parámetros de seguridad/veracidad establecidos mediante la regulación de los nodos involucrados, la invención reivindicada en la presente solicitud proporciona una metodología de configuración técnica de *un libro mayor electrónico, de bloques interconectados, de un sistema de cadena de bloques, de uno o más nodos (denominados de billetera), y de uno o más nodos de construcción de bloques*, con el objetivo de la implementación de un proceso (***proceso de propagación de datos de confiar, pero verificar***) en donde al menos un nodo de construcción de bloques está configurado para crear al menos un nuevo bloque interconectado en el sistema de cadena de bloques antes de verificar la corrección de uno o más bloques precedentes, lo cual no se encuentra divulgado en el arte previo citado.

Ahora bien, el examinador establece que la diferencia con 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”*. En este sentido, me permito resaltar que el proceso de propagación de datos de **confiar, pero verificar**, se utiliza para determinar cuál de los bloques o cadenas que compiten se agrega a la cadena de bloques o al libro mayor distribuido, y cuál de los nodos que compiten se selecciona para recibir una recompensa por el bloque o cadena que se agrega a la cadena de bloques o al libro mayor distribuido, el cual **aumenta significativamente el rendimiento transaccional de los sistemas actualmente conocidos al reducir las restricciones de linealidad (y otras restricciones informáticas que retrasan el procesamiento general del sistema) y permite que el rendimiento de procesamiento del sistema se aproxime al rendimiento máximo teórico para cadenas de bloques y sistemas de libro mayor electrónico distribuido en general.**

En segundo lugar, con respecto al arte previo citado, me permito señalar que **D1** se dirige a un sistema de consenso para cadenas de bloques que carecen de una autoridad central de confianza. También establece que la pluralidad de dispositivos conectados a la red puede entonces determinar un candidato principal para enviar un siguiente bloque de datos para agregar o anexas al libro de contabilidad distribuido, utilizando un criterio de selección que puede comprender seleccionar un minero cuyo mensaje de anuncio produzca uno de los siguientes: una diferencia más pequeña, una diferencia más grande, una diferencia más cercana a un valor objetivo, una diferencia más cercana al valor objetivo módulo una constante, una diferencia calculada utilizando una función que toma como entrada el valor de la salida hash y el valor del hash de la clave pública y el identificador de dirección único.

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, si un experto en la materia combinara las enseñanzas de **D3** con **D1**, no podría ni llegaría a las **características diferenciadoras** descritas en la reivindicación 1 de la presente solicitud.

Por otro lado, el examinador afirma que **D1** enseña “*un sistema de consenso y un método para agregar datos a una cadena de bloques*” y que **D1** “*es un documento relacionado con el estado de la técnica*”, por lo tanto, es relevante para objetar la patentabilidad de la presente solicitud. Sin embargo, y contrario a lo establecido por el examinador, me permito señalar mi total desacuerdo con respecto a la relevancia de **D1**, como se explica a continuación.

Como se puede observar en el párrafo [0032] de **D1**, el cual revela que “*La pluralidad de dispositivos conectados a la red puede entonces determinar **un candidato principal para enviar un siguiente bloque de datos** para añadirlo o anexoarlo al libro mayor distribuido; utilizando un criterio de selección que puede comprender **la selección de un minero** cuyo mensaje de anuncio produzca uno de...*”, me permito señalar que la entidad seleccionada aquí es un minero, es decir, un nodo de red, tal como se establece en el párrafo [0011] de **D1**: “*un nodo validador o 'minero'*”, el cual es elegido para la función de enviar el siguiente bloque de datos a la cadena de bloques. No obstante, **D1** no parece divulgar ningún proceso en el que se seleccionen bloques candidatos. Más bien, **D1** parece referirse únicamente a la selección de un nodo que luego envía el siguiente bloque. Por lo tanto, incluso si un experto en la materia consultara **D1** y considerara adaptar a **D3** basándose en las enseñanzas de **D1**, no llegaría ni obtendría la invención reclamada en la presente solicitud.

Por otro lado, y con el fin de “*curar*” las deficiencias de **D1**, el examinador cita el documento **D3**, el cual está dirigido de forma general con un esquema de cadena de bloques llamado OmniLedger, que corresponde a “*un novedoso libro mayor distribuido escalable que preserva la seguridad a largo plazo bajo operación sin permisos*” (**D3**, Resumen). En particular, en la Página 2, Columna 1, Tercer párrafo de **D3** se enseña que “*para minimizar la latencia de las transacciones en casos comunes, como los pagos de bajo valor, 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. Este enfoque de dos niveles garantiza que cualquier comportamiento incorrecto dentro del primer nivel se detecte en minutos y pueda desincentivarse enérgicamente mediante recursos como la pérdida de depósitos. Los clientes pueden esperar a que ambos niveles procesen las transacciones de alto valor para obtener la máxima seguridad o simplemente esperar a que el primer nivel procese las transacciones de bajo valor*” (negrilla fuera de texto).

Además, en la Página 8, Columna 2 de **D3** se proporcionan más detalles sobre el esquema “*confiar pero verificar*” divulgado en **D3**, en donde se describe que “*En respuesta a las necesidades de los clientes, aumentamos la arquitectura intra-shard (ver Figura 4) siguiendo un modelo de ‘confiar, pero verificar’, en donde los validadores optimistas procesan las transacciones rápidamente, proporcionando un compromiso provisional pero poco probable de cambiar, y los validadores centrales verifican posteriormente de nuevo la transacción para proporcionar finalidad y garantizar la verificabilidad (...) Como resultado, es posible que se confirmen algunas transacciones erróneas, pero, en última instancia, los validadores centrales verifican todos los compromisos provisionales, detectando cualquier inconsistencia y a sus responsables*”, y asimismo que “*Las transacciones son procesadas primero por un grupo optimista que produce bloques validados de forma optimista. Estos bloques sirven como entrada para la revalidación por parte de los validadores centrales, que se ejecutan simultáneamente y combinan las entradas de múltiples grupos de procesamiento optimistas (...) Las transacciones válidas se incluyen en un bloque finalizado que se añade al libro mayor del shard y finalmente se incluyen en el bloque de estado*” (negrilla fuera de texto).

De acuerdo con lo anterior se evidencia que, aunque **D3** utiliza el término “*confiar, pero verificar*”, el esquema así descrito **no** es el mismo que el reclamado en la reivindicación 1. En particular, el esquema de **D3** parece centrarse en proporcionar un resultado de verificación rápido y provisional, para luego confirmar o revocar este resultado provisional mediante un segundo paso de verificación, más confiable pero más lento. Por lo cual, el objetivo de este proceso parece ser proporcionar algún tipo de resultado de verificación (aunque no sea totalmente confiable) lo más rápidamente posible.

Sin embargo, **D3** no revela ningún esquema en el que se inicie el trabajo en un bloque siguiente antes de finalizar el proceso de verificación. Como se observa, **D3** simplemente indica (como se mencionó anteriormente) que cada bloque está sujeto a dos niveles de validación antes de ser añadido a la cadena de bloques, pero no revela el inicio de ningún otro proceso mientras tanto, y mucho menos el inicio del trabajo en un nuevo bloque antes de la verificación del bloque anterior. Por lo cual, respetuosamente consideramos que el uso aparentemente coincidente del mismo término, “*confiar, pero verificar*”, para describir **dos procesos diferentes con dos objetivos diferentes**, tal como se ha descrito anteriormente, no debería significar que los dos procesos se fusionen, y por lo tanto, un experto en la materia

no podría llegar a la materia reivindicada en la presente solicitud de forma obvia a partir de las enseñanzas de **D3**.

En consecuencia, me permito resaltar que **D3** no divulga al menos la siguiente característica mencionada en la reivindicación 1 actualmente reclamada:

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 (negrilla fuera de texto)

En este sentido, el efecto técnico de esta característica diferenciadora es que, una vez completada la verificación, siempre que al menos uno de los bloques verificados sea confiable, ya se habrá comenzado a trabajar en el siguiente bloque de la cadena de bloques, el cual, por lo tanto, estará listo más rápidamente. De este modo, **el rendimiento del sistema** (en el sentido de la velocidad a la que se pueden añadir bloques) **aumenta a lo largo de muchas transacciones**.

Adicionalmente, me permito señalar que, cuantos más bloques competidores se implementen en una determinada realización, mayor será la probabilidad de que uno de ellos se verifique correctamente, lo que se traduce en el ahorro de tiempo descrito anteriormente. En otras palabras, se utiliza el procesamiento en paralelo para permitir una ventaja inicial en el siguiente bloque antes de que se complete la verificación del bloque anterior. Aún más, me permito resaltar que este efecto técnico se describe con más detalle, por ejemplo, en los Párrafos [0008] y [0194] - [0205] de solicitud PCT, los cuales establecen que:

*[0008] Otro objeto y una característica de la presente invención es la implementación de un consenso de Gradiente de Idoneidad o una variante que incorpora la metodología de “**confiar, pero verificar**” para determinar cuál de los bloques o cadenas que compiten se agrega a la cadena de bloques o al libro mayor distribuido, y cuál de los nodos que compiten se selecciona para recibir una recompensa por el bloque o cadena que se agrega a la cadena de bloques o al libro mayor distribuido. Esta estrategia aumenta significativamente el rendimiento transaccional de los sistemas actualmente conocidos al reducir las restricciones de linealidad (y otras*

restricciones informáticas que retrasan el procesamiento general del sistema) y permite que el rendimiento de procesamiento del sistema se aproxime al rendimiento máximo teórico para cadenas de bloques y sistemas de libro mayor electrónico distribuido en general.

[0194] Una limitación importante de los sistemas de la cadena de bloques de prueba de trabajo conocidos (y de muchos sistemas de prueba de participación) es su linealidad. Debido a que la salida de cada transacción puede actuar como la posible entrada de cada transacción subsecuente, todas las operaciones deben ejecutarse secuencialmente y todos los registros deben ordenarse de manera determinista. Además, la cadena de bloques se organiza como una cadena vinculada - una secuencia lineal de nodos. Por lo tanto, solamente puede crearse un nuevo bloque una vez que se conocen los bloques precedentes.

[0195] Bajo la restricción de linealidad, el rendimiento máximo de cualquier cadena de bloques puede proyectarse teóricamente como el número de operaciones y registros que pueden procesarse en secuencia mediante un programa que se ejecuta en un solo hilo en una computadora. En dependencia del hardware y el software usados, esto puede ser cientos de miles o millones de operaciones por segundo - lo que puede traducirse en muchos miles de transacciones por segundo, en dependencia de la complejidad informático de las transacciones individuales.

[0196] Además, en realidad, el rendimiento real observado varía significativamente de este máximo teórico. Un número de razones diferentes explican esta diferencia y explican por qué las implementaciones conocidas de la cadena de bloques no pueden lograr este rendimiento máximo teórico.

[0197] En los sistemas conocidos de consenso de prueba de trabajo, la mayor parte de los recursos informáticos se dedican a resolver el problema de la prueba de trabajo. Calcular la prueba de trabajo crea un retraso, pero este retraso es tratado por estos sistemas como una característica en lugar de un defecto. La dificultad de la prueba de trabajo se dirige a un retraso de tiempo específico entre los bloques, y la dificultad se ajusta para sincronizarse con ese retraso de tiempo.

[0198] Los sistemas conocidos de consenso de prueba de participación, así como también los sistemas de consenso basados en la votación y la aprobación, se toman el

tiempo para coordinar entre los nodos, a fin de decidir qué nodo se autoriza a crear un nuevo bloque. En la práctica, estos enfoques permiten un tiempo de creación de bloques mucho más rápido y un mayor rendimiento de las transacciones que los sistemas de prueba de trabajo, pero típicamente a expensas de requerir algún tipo de centralización.

[0199] Aun así, incluso en estos sistemas, la cantidad de tiempo necesario para establecer el consenso no es trivial, ya que requiere los nodos para sincronizar su estado. Además, la mayoría de estos sistemas generan cierto retraso entre los bloques (durante el consenso y la creación), para proporcionar suficiente tiempo para permitir la propagación de datos.

[0200] El retraso entre los bloques permite que los registros de datos y los bloques descubiertos se propaguen a través de la red, típicamente a través de un protocolo gossip. Entre estas dos categorías de datos, las transacciones constituirán la mayor proporción.

[0201] Cuando se crea y distribuye un nuevo bloque, los nodos dentro de la red validarán el bloque al ejecutar las transacciones que contiene. Una variación de “confiar, pero verificar” del consenso de Gradiente de Idoneidad de acuerdo con al menos una modalidad pretende eliminar o reducir varias de las restricciones conocidas de las implementaciones de la cadena de bloques conocidas, y permitir que el procesamiento del sistema de la cadena de bloques práctico se aproxime al rendimiento máximo teórico (discutido anteriormente).

*[0202] Un ejemplo de la propagación del bloque de propagación mediante el uso de la variación “**confiar, pero verificar**” del consenso de Gradiente de Idoneidad de acuerdo con al menos una modalidad de la invención se describe más abajo con referencia a las **Figuras 12A-D y 13A-B**.*

[0203] En al menos una modalidad, la presente invención seguirá ejecutando las operaciones de las cadenas de bloques linealmente, pero usará y aprovechará los sistemas informáticos multiprocesador/multinúcleo/multicpu (o clústers) al realizar el procesamiento de validación en una implementación de software paralela y multihilo (o multiproceso). En al menos una modalidad de la presente invención, cada una de

las siguientes actividades puede ocurrir de manera simultánea y en gran medida independiente de las otras actividades:

- (a) el hilo principal de construcción de bloques, proceso o corutina construye sobre el bloque de mayor Idoneidad conocido por el nodo de entre los bloques ya difundidos a la red;*
- (b) un hilo, proceso o corutina continúa en base al mejor bloque anterior propio del nodo que se produjo por sí mismo (con validación y confirmación inherentes) en caso de que el hilo, proceso o corutina “ganador” no pueda validarse (es decir, es fraudulento);*
- (c) uno o más hilos/procesos en paralelo se basan en el bloque secundario, o un bloque de descubrimiento tardío, como otra copia de seguridad del bloque de mayor Idoneidad;*
- (d) uno o más hilos/procesos en paralelo adquieren de nodos pares todas las transacciones de bloques adquiridos externamente, y luego proceden a validar esos bloques.*

[0204] Mediante el uso de esta metodología de consenso de Gradiente de Idoneidad de la presente invención, un nodo enfrenta un gran riesgo de que los esfuerzos de construcción de bloques se desperdicien en caso de que se adopte un bloque fraudulento y no verificable como la base sobre la cual comenzar a construir el siguiente bloque. Tal bloque fraudulento deberá desecharse, junto con cualquier trabajo realizado para construir sobre él.

[0205] Sin embargo, siempre que la incidencia de fraude sea baja, luego el rendimiento de la implementación de acuerdo con al menos una modalidad de la presente invención correspondería a la velocidad de los hilos/procesos que trabajan para construir el siguiente bloque. Incluso estar dentro de uno o dos órdenes de magnitud del rendimiento máximo teórico haría que la variación de consenso de Gradiente de Idoneidad de la presente invención, mediante el uso del método de propagación de datos de “confiar, pero verificar”, fuera más eficiente y de mejor rendimiento (con respecto al rendimiento) que las implementaciones existentes de la cadena de bloques.

De acuerdo con lo anterior, el problema técnico objetivo resuelto por la reivindicación 1 es ***cómo modificar D3 para aumentar el rendimiento del sistema de cadena de bloques***, lo cual es **completamente diferente** a lo establecido por el examinador en el Oficio que se contesta, en donde indica que *“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?”*.

Por otro lado, se evidencia claramente que **D3** enseña que el esquema de “*confiar pero verificar*” de este documento, tiene como objetivo “*maximizar el rendimiento del sistema*”, tal como se describe en el último párrafo de la Página 8, Columna 2, y, por lo tanto, un experto en la materia que use **D3** con el objetivo de realizar modificaciones para mejorar el rendimiento puede considerar cómo se podría optimizar aún más dicho esquema de confiar pero verificar divulgado en **D3**.

Ahora bien, como se indicó anteriormente, el esquema de “*confiar pero verificar*” de **D3** es **diferente** del esquema de “*confiar, pero verificar*” de la reivindicación 1 de la presente solicitud. Específicamente, **D3** no proporciona ninguna sugerencia o enseñanza sobre un esquema en el que el trabajo en el siguiente bloque se inicie antes de que finalice el proceso de verificación, sino que se centra en proporcionar resultados de verificación anticipados como método para mejorar el “*rendimiento*” (tal y como se utiliza el término en **D3**). Por lo tanto, un experto en la materia que use **D3** considerando el problema técnico objetivo descrito, no tendría motivos o razones para considerar modificaciones en la **característica diferenciadora antes identificada**.

Aún más, un experto en la materia definiría “*rendimiento*” en el contexto de una cadena de bloques como la tasa de producción de nuevos bloques, multiplicada por el número de transacciones en cada nuevo bloque, expresada en términos del número promedio de transacciones procesadas por segundo. Por lo cual, y a pesar de las enseñanzas de **D3**, este documento no enseña ni sugiere ninguna forma por la cual dicho “*rendimiento*” podría producirse más rápido utilizando el algoritmo especificado; de hecho, dado que la etapa optimista y la etapa de finalización del algoritmo especificado necesitan ejecutarse en secuencia para cada bloque, es probable que **el rendimiento global sea menor, no mayor, que el de otras alternativas**.

Por el contrario, el algoritmo actualmente reclamado en la reivindicación 1 permite una mejora significativa en el rendimiento, debido a que cada nuevo bloque que se construye puede comenzar a construirse inmediatamente después de que se haya construido el bloque anterior, y una etapa de validación no contribuye al tiempo total que se tarda en construir un nuevo bloque, lo que resulta en un aumento significativo del rendimiento.

Considerando lo anteriormente expuesto, se puede concluir que, **D3** 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 **D3** 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 **D3**.

En tercer lugar, considerando lo indicado en el Manual para el Examen de Solicitudes de Patentes de Invención en las Oficinas de Propiedad Industrial de los países de la Comunidad Andina que establece que *“Para juzgar si la invención definida por las reivindicaciones realmente se deriva de manera evidente del estado de la técnica, hay que determinar si carece de nivel inventivo cuando se consideran las diferencias entre ésta y el estado de la técnica más cercano. El examinador tiene la carga de probar que la invención carece de nivel inventivo y no sólo limitarse a establecer las diferencias entre la solicitud y dicho estado de la técnica”* (subrayado y negrilla fuera de texto), me permito llamar la atención de ese Despacho en el hecho que cada invención es de cierta medida una combinación de elementos relacionados entre sí, por lo que no es suficiente afirmar que dichos elementos y/o características ya habían sido previamente divulgados, partiendo de combinaciones de enseñanzas convenientes, y que por ende, la combinación de fracciones de diferentes documentos permiten la deducción obvia de la invención reclamada, por lo tanto, el examinador debe demostrar con argumentos válidos, **por qué** un experto en la técnica habría llegado a la invención reivindicada de **forma obvia** basándose en las enseñanzas de **D1** y **D3**.

Así las cosas, es claro que el Examinador basó su análisis solo en la comparación de las diferencias de la presente solicitud con el documento **D1** y la búsqueda de otro documento que “**curara**” dichas diferencias. Además, el hecho de que un experto en la materia pueda modificar las características específicas necesarias, como lo asume el Examinador, para llegar al objeto reivindicado no significa que el experto en la materia lo haría con la expectativa de alguna mejora, ya que en ninguno de los documentos citados se sugieren los mismos elementos y características del método implementado por computador reivindicado en la presente solicitud, ni mucho menos los efectos que este tendría.

Además, **D1** y **D3** no establecen una mínima indicación de qué modificaciones debería efectuar una persona versada en la materia para poder obtener el método implementado por computador aquí reclamado de acuerdo con el nuevo Capítulo Reivindicatorio adjunto a este memorial.

De esta forma, me permito señalar que la sola similitud entre el método reclamado y aquellos del arte previo (*si es que la hay*) es **insuficiente** para determinar o concluir una supuesta falta de nivel inventivo y consideramos entonces que en un juicioso análisis de nivel inventivo **debió haber alguna razón o motivación** que hubiese llevado a un experto en la técnica a **modificar el estado de la técnica más cercano para llegar a la invención reivindicada de forma obvia**. Hacemos énfasis también en que el examinador no ha proporcionado ninguna evidencia o razón válida por la cual un experto en la técnica se habría sentido **motivado** a realizar las modificaciones necesarias a los métodos de la técnica anterior para llegar de forma obvia a la presente invención.

Por lo tanto, el análisis de nivel inventivo de solicitudes de patente, no se trata de encontrar en el arte previo **una simple invitación a experimentar con uno o más cambios aleatorios**, sino de identificar en los documentos citados una enseñanza y guía específica para hacer las modificaciones necesarias **que lo lleven con certeza** a la materia reclamada, lo cual no sucede en este caso. Por lo cual, la materia reivindicada en la nueva reivindicación **1** difiere de gran manera con aquella divulgada en el arte previo y, por tanto, es inventiva a la luz de las enseñanzas de **D1** y **D3**.

Por cualquiera de las razones anteriores, es más que evidente que el análisis de nivel inventivo no puede ser basado en un estándar “*posible de alcanzar*”, debido a que esto haría que toda invención fuera no patentable. Así, como se resalta en el Artículo 18 de la Decisión 486, las invenciones deberían considerarse como inventivas cuando la materia reclamada no

puede ser derivada del arte previo. Adicionalmente, la presente invención es inventiva a la luz de los documentos citados, pues siguiendo las enseñanzas de **D1 y D3**, la persona medianamente versada en la materia no obtendría la materia modificada y aquí reclamada, ni podría esperar que ésta presentase los efectos presentados y que se han discutido anteriormente.

Así las cosas, y en vista de lo anteriormente expuesto, respetuosamente solicito el retiro de las objeciones de la presente solicitud y la concesión del privilegio solicitado, ya que en opinión del solicitante cumple con todos los requisitos establecidos en la Decisión 486.

3. Anexos

- Capítulo Reivindicatorio Modificado
- Tasa Oficial de modificación a las reivindicaciones
- Tasa Oficial por 1 reivindicación adicional

JUAN PABLO CADENA SARMIENTO

T.P. No. 57.492 del C.S.J.
C.C. 80.410.337 de Usaquén
Calle 70 A No. 4 – 41



REIVINDICACIONES MODIFICADAS

1. Un método implementado por computador en una red informática, comprendiendo el método implementado por computador:

configurar un libro mayor electrónico distribuido en una memoria electrónica (114) de una o más computadoras (110) en un sistema de cadenas de bloques (100), 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;

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 de datos refleje una transformación de al menos una parte de un estado global del libro mayor electrónico distribuido;

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);

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;

configurar el uno o más nodos de construcción de bloques (110) para construir uno o más nuevos 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; 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.

2. El método implementado por computador de la reivindicación 1, en donde el proceso de propagación de datos de confiar, pero verificar incluye además propagar dicho al menos un nuevo bloque interconectado en el sistema de cadenas de bloques (100) a través de una red de intercambio de datos.

3. El método implementado por computador de la reivindicación 2, en donde dicho al menos un nuevo bloque interconectado se propaga a través del sistema de cadenas de bloques (100), que además incluye:

transmitir dicho al menos un nuevo bloque interconectado como un encabezado de bloque, mientras que se excluye la mayor parte de los datos pertenecientes a dicho al menos un nuevo bloque interconectado.

4. El método implementado por computador de la reivindicación 2, en donde dicho al menos un nuevo bloque interconectado se propaga a través del sistema de cadenas de bloques (100), que además incluye:

transmitir dicho al menos un nuevo bloque interconectado sin que uno o más registros de datos pertenezcan a dicho al menos un nuevo bloque interconectado, dichos uno o más registros de datos transmitidos por separado de dicho al menos un nuevo bloque interconectado.

5. El método implementado por computador de la reivindicación 1, que además incluye:

al menos otro nodo de construcción de bloques (110) creando al menos un siguiente bloque interconectado encima de dicho al menos un nuevo bloque interconectado después de que dicho al menos un nuevo bloque interconectado se distribuye al sistema de cadenas de bloques; y

el al menos otro nodo de construcción de bloques creando simultáneamente el al menos un siguiente bloque interconectado mientras que uno o más registros de datos pertenecientes a dicho al

menos un nuevo bloque interconectado son descargados por el al menos otro nodo de construcción de bloques, o mientras dicho al menos un nuevo bloque interconectado se valida.

6. El método implementado por computador de cualquiera de las reivindicaciones 1 a 5, en donde el proceso de propagación de datos de confiar, pero verificar incluye además hacer que el al menos un nodo de construcción de bloques (110) incluya un filtro Bloom en un encabezado del bloque de dicho al menos un nuevo bloque interconectado en el sistema de cadenas de bloques (100), de modo que el proceso de propagación de datos de confiar, pero verificar hace que el al menos un nodo de construcción de bloques (110) distribuya el filtro Bloom con el al menos un nuevo bloque interconectado en el sistema de cadenas de bloques (100).

7. El método implementado por computador de la reivindicación 6, en donde el filtro Bloom está configurado para representar un conjunto de cuentas contables electrónicas distribuidas u otros datos afectados u operados durante uno de (i) la creación, (ii) la validación, o (iii) la ejecución de dicho al menos un nuevo bloque interconectado en el sistema de cadenas de bloques (100).

8. El método implementado por computador de la reivindicación 6, en donde el filtro Bloom de un bloque es una estructura de datos configurada al menos

con la propiedad de que cualquier cuenta u otros datos encontrados en el filtro Bloom es posible o probable que tenga un estado de la cuenta u otros datos modificados por la validación y ejecución del bloque, o que haya sido operado o afectado de otra manera por el bloque o por registros de datos pertenecientes a el bloque, y

con la propiedad de que cualquier cuenta que no se encuentre en el filtro Bloom seguramente no cambiará en cuanto a el estado de la cuenta que no se encuentre en el filtro Bloom, o no se verá afectada por el bloque o por los registros de datos que pertenecen al bloque.

9. El método implementado por computador de la reivindicación 8, en donde crear dicho al menos un nuevo bloque interconectado incluye, además:

identificar cuentas afectadas u operadas cuando se ejecutan uno o más contratos inteligentes, o cuando se agregan uno o más registros de datos a dicho al menos un nuevo bloque interconectado;

comprobar para asegurar que cada cuenta identificada no esté contenida dentro de un filtro Bloom de al menos un bloque interconectado anterior que precede a dicho al menos un nuevo bloque interconectado; y

si una cuenta identificada está contenida dentro de un filtro Bloom del al menos un bloque interconectado anterior, detener la ejecución de dicho uno o más contratos inteligentes o detener la inclusión de dicho uno o más registros de datos, y descartar dicho uno o más contratos inteligentes o uno o más registros de datos de dicho al menos un nuevo bloque interconectado.

10. El método implementado por computador de cualquiera de las reivindicaciones 1 a 9, en donde el proceso de propagación de datos de confiar, pero verificar utiliza la estructura de datos de gráficos acíclicos dirigidos (DAG) para disponer dicho al menos un nuevo bloque interconectado.

11. El método implementado por computador de la reivindicación 10, en donde el proceso de propagación de datos de confiar, pero verificar permite que dicho al menos un nuevo bloque interconectado tenga referencias posteriores a uno o más bloques interconectados (210A, 210B, 210C) o subcadenas en el sistema de cadenas de bloques (100), provocando que al menos una parte del libro mayor electrónico distribuido constituya un gráfico acíclico dirigido (DAG).

12. El método implementado por computador de la reivindicación 11, en donde el proceso de propagación de datos de confiar, pero verificar asegura que los múltiples bloques interconectados (210A, 210B, 210C) o subcadenas que se construyen simultáneamente por dicho nuevo bloque interconectado incluyen registros asociados con conjuntos distintos y mutuamente excluyentes de cuentas u otros datos, de modo que los múltiples bloques interconectados o subcadenas que se construyen afectan a conjuntos de cuentas mutuamente excluyentes u otros datos.

13. El método implementado por computador de la reivindicación 12, en donde el proceso de propagación de datos de confiar, pero verificar permite que los múltiples bloques interconectados

(210A, 210B, 210C) o subcadenas se comparen rápidamente para determinar si alguno de los múltiples bloques interconectados o subcadenas opera en cuentas comunes u otros datos.

14. El método implementado por computador de la reivindicación 12, que además incluye una etapa de comparar los respectivos filtros Bloom de los múltiples bloques interconectados (210A, 210B, 210C) o subcadenas para determinar con certeza que los bloques interconectados o subcadenas en el sistema de cadenas de bloques (100) afectan u operan sobre conjuntos de cuentas mutuamente excluyentes u otros datos.

15. El método implementado por computador de la reivindicación 1, en donde el proceso de propagación de datos de confiar, pero verificar permite la creación simultánea de una pluralidad de nuevos bloques interconectados en el libro mayor electrónico distribuido, de modo que múltiples nodos en el sistema de cadenas de bloques (100) están creando uno o más de la pluralidad de nuevos bloques interconectados en paralelo; y

en donde el proceso de propagación de datos de confiar, pero verificar garantiza que los registros de datos no se propaguen ampliamente a través del sistema de cadenas de bloques (100) antes de la creación de bloques interconectados, de modo que los registros de datos producidos por un nodo determinado solo se comparten con otros nodos determinados dentro del sistema de cadenas de bloques (100); y

en donde el proceso de propagación de datos de confiar, pero verificar garantiza que un nodo de construcción de bloques (110) respectivo solo cree dicho al menos un nuevo bloque interconectado utilizando registros de datos propagados por ciertos nodos dentro del sistema de cadenas de bloques (100).

16. El método implementado por computador de la reivindicación 1, en donde si un nodo de construcción de bloques (110) descubre que dicho al menos un nuevo bloque interconectado no se puede validar, dicho al menos un nuevo bloque interconectado se descarta junto con cualquier bloque nuevo o subsiguiente que se construya sobre dicho al menos un nuevo bloque interconectado; y

en donde un bloque no se puede validar si ocurre uno de los siguientes: (i) una raíz de árbol Merkle (225A-D) no se puede reproducir utilizando un conjunto de registros de datos (220A-C) que pertenecen a dicho bloque en el sistema de cadenas de bloques (110), (ii) un hash de bloque (240A-C) en dicho bloque se especifica incorrectamente, o (iii) un registro de datos perteneciente a dicho bloque no es válido o viola una regla en el sistema de cadenas de bloques.

17. El método implementado por computador de las reivindicaciones 1 a 16, en donde el sistema de cadena de bloques (110) impone un retraso de tiempo entre el al menos un nuevo bloque interconectado y al menos un bloque interconectado subsecuente al requerir un espacio mínimo de tiempo entre bloques.

18. El método implementado por computador de la reivindicación 17, en donde el espacio mínimo de tiempo entre bloques es un segmento de tiempo cuantificado por un número mínimo de unidades informáticas para ejecutarse en secuencia.

19. El método implementado por computador de cualquiera de las reivindicaciones 1 a 18, en donde el proceso de propagación de datos de confiar, pero verificar aumenta el rendimiento de transacciones del sistema de cadenas de bloques (100) en relación con el rendimiento de transacciones de un sistema de cadenas de bloques de prueba de trabajo de consenso de Nakamoto.

20. El método implementado por computador de cualquiera de las reivindicaciones 1 a 19, en donde el al menos un nodo de construcción de bloques (110) es un nodo de construcción de bloques identificable configurado con una dirección de recompensa que se incluye con al menos un bloque interconectado sujeto que está siendo construido por dicho al menos un nodo de construcción de bloques identificable; y

en donde dicho al menos un bloque interconectado sujeto es un bloque firmado criptográficamente por dicho al menos un nodo de construcción de bloques identificable que utiliza al menos una clave criptográfica asociada con dicha dirección de recompensa,

en donde el al menos un bloque firmado se propaga en la red de cadena de bloques.

21. El método implementado por computador de la reivindicación 20, en donde al menos otro nodo de construcción de bloques (110) implementa un proceso de evaluación de confianza, mediante el cual, dicho al menos otro nodo de construcción de bloques, al recibir dicho bloque firmado, determina si generar un nuevo bloque subsiguiente que se basa en dicho bloque firmado o encabezado de bloque antes de que dicho bloque firmado o encabezado de bloque sea validado;

en donde el proceso de evaluación de confianza incluye además evaluar si dicha dirección de recompensa ha firmado algún bloque anterior propagado previamente en la red de cadena de bloques, y en donde dichos bloques anteriores firmados por dicha dirección de recompensa son válidos o no válidos.

22. El método implementado por computador de la reivindicación 20, en donde configurar el proceso de propagación de datos de confiar, pero verificar incluye además al menos uno de:

(a) configurar el bloque firmado para especificar una tarifa de construcción como una cantidad de tokens de libro mayor electrónico distribuidos, cuyo bloque firmado está configurado como un bloque incentivado, y al menos otro nodo de construcción de bloques genera un nuevo bloque posterior configurado con una referencia a dicho bloque incentivado;

en donde la tarifa de construcción de bloques incentivada se transfiere desde la dirección de recompensa a una dirección de libro mayor distribuida especificada por el al menos otro nodo de construcción de bloques; o

(b) configurar el bloque firmado para especificar tokens en riesgo como una cantidad de tokens de libro mayor electrónico distribuidos, cuyo bloque firmado funciona como un bloque garantizado, y configurar al menos otro nodo en la red de cadena de bloques construye un registro de penalización que contiene o hace referencia al bloque garantizado,

cuyo registro de penalización, cuando se incorpora a un nuevo bloque posterior, hace que los tokens en riesgo especificados se transfieran desde la dirección de recompensa a una dirección de libro mayor

distribuida especificada por el al menos otro nodo en la red de cadena de bloques, si el bloque garantizado es inválido.