

Cra. 43A # 1- 50 Of. 209
San Fernando Plaza
Medellín, Colombia
Tel: +574 444 3815

3. ARGUMENTOS A FAVOR DE LA NOVEDAD Y NIVEL INVENTIVO DE LA SOLICITUD

3.1. El señor Examinador afirma que el objeto reclamando en las reivindicaciones 1 a 5 carece de novedad a la luz de las enseñanzas de D1 y que el objeto de las reivindicaciones 6 a 10 carece de nivel inventivo en virtud de las enseñanzas de D1 y D2.

3.2. El Solicitante respetuosamente se encuentra en desacuerdo con dichas afirmaciones.

3.3. La primera referencia citada D1 describe métodos para administrar o registrar eventos después de que ocurrieron esos eventos, en donde el sistema que procesa el evento pasa la información de registro del evento a otro sistema que se encarga de registrar dicho evento. La segunda referencia citada D2 describe un método para establecer comunicaciones seguras entre dos dispositivos en una red doméstica inteligente.

3.4. La invención reclamada por el Solicitante procesa una transacción y genera y graba el registro o auditoría de esa transacción al mismo tiempo en el mismo proceso. Elimina cualquier brecha temporal entre una transacción o evento, por un lado, y el registro o auditoría, por el otro. Hasta ahora, cada sistema primero ha procesado una transacción o evento, y luego ha pasado un registro de esa transacción o evento al sistema de registro o auditoría, que luego crea un registro o auditoría de esa transacción o evento. Ese retraso representa la brecha temporal que elimina la invención en cuestión.

3.5. El estado de la técnica se ha centrado, hasta la presente solicitud, en asegurar una cadena de auditoría (ver, por ejemplo, el párrafo [0001] en D1) o en establecer un enlace de comunicaciones seguro entre dos o más dispositivos (ver, por ejemplo, el párrafo [0002] en D2). No se ha centrado en eliminar la brecha temporal entre el momento en que un sistema procesa un evento o transacción y el momento en que ese sistema procesa posteriormente el registro o la auditoría de esa transacción o evento, ya que hasta ahora se pensaba que esto era imposible de lograr. Esa brecha temporal ha dado lugar a muchos problemas con la creación de sistemas escalables en tiempo real, ya que una falla del sistema puede llevar a que el registro de ese evento o transacción se pierda o se corrompa antes de agregarlo al registro o al proceso de auditoría. Al eliminar esa brecha temporal, el sistema reclamado elimina esos problemas y esto conduce a la capacidad de crear sistemas escalables en tiempo real que son mucho más eficientes y robustos que los diseñados con la técnica anterior.

3.6. Los documentos citados no implican que una auditoría pueda generarse al mismo tiempo que la transacción en sí. El documento D1 establece explícitamente que los sistemas reciben un evento de transacción, esta es la transacción procesada, y luego genera y almacena el registro

de ese evento. El hecho de que las transacciones puedan o no estar firmadas es irrelevante para el hecho de que sus registros se crean después de que la transacción ha sido procesada. Esa brecha de tiempo, sin importar cuán pequeña sea, entre el momento en que se procesa una transacción y la hora en que se registran y graban las transacciones, presenta la brecha temporal que brinda una ventana de oportunidad para que esa transacción se pierda o altere antes de que se registre. Las reivindicaciones en D1 simplemente intentan dificultar la intromisión en una pista de auditoría existente. No eliminan la brecha temporal entre una transacción o evento y la pista de auditoría de esa transacción o evento. Las reivindicaciones en D2 son aún más limitadas e intentan establecer comunicaciones seguras entre dos dispositivos cuando el nivel de seguridad es un compromiso entre el nivel de seguridad y la velocidad de procesamiento requerida para configurar esa comunicación. En ninguna parte se relacionan con el procesamiento de una pista de auditoría o con la eliminación de la brecha temporal entre una transacción o evento y la pista de auditoría de esa transacción o evento.

3.7. Ahora bien, D1 da a conocer un método de registro de eventos [0001] para proteger, verificar y redactar registros informáticos. Se describe un sistema de registro en el que, en diversas realizaciones, el sistema puede recibir eventos para registrar y almacenar los eventos registrados en una estructura de datos de registro verificable y redactable. En una realización, un evento se registra de manera que la entrada del registro de eventos incluye múltiples cadenas de caracteres pseudoaleatorias que dependen de la entrada del registro, al menos una de las cuales también depende de las entradas del registro anteriores. En algunas realizaciones, el registro se puede redactar mientras se mantiene su estructura verificable sin permitir que un atacante determine posibles entradas de registro que se ajusten a los eventos redactados. Para ayudar en la usabilidad del registro, se puede emplear una firma digital con sello de tiempo por un servidor de tiempo confiable para crear puntos de control de registro y permitir la segmentación del registro. En un escenario, las firmas digitales con sello de tiempo pueden basarse en claves efímeras de independientes. Otra característica posible del sistema de registro puede ser emplear el anidamiento de eventos de registro para objetos particulares para detectar la manipulación o eliminación de las entradas de registro del objeto [0021]. Revela que un servidor de registro recibe mensajes o eventos de un sistema después de que ese sistema ha generado esas transacciones o eventos [0104] donde el servidor de registro genera los valores hash de ese mensaje o evento [0105]. El sistema calcula al menos dos hash para cada evento, un hash de registro y un hash de resumen [0057] a [0059], donde luego los agrega al registro, junto con los metadatos que rodean ese evento. La referencia describe además que un sistema informático puede calcular múltiples

hash (reivindicación 11) para un evento, y donde puede generar un registro hash que se relaciona con múltiples eventos (reivindicación 10).

3.8. Por otro lado, D2 describe un método para establecer comunicaciones entre dos nodos de redes inteligentes [0003]. Revela métodos y sistemas para establecer comunicaciones seguras hacia y/o desde dispositivos en una red de malla inteligente. Las realizaciones incluyen el establecimiento de una sesión de comunicación cifrada utilizando una clave de cifrado derivada de una solicitud de sesión utilizando una combinación de clave pública y clave privada [0006]. Cuando un respondedor dentro de la red recibe una solicitud para comenzar una sesión, el respondedor valida la solicitud. Una vez validado, se proporciona una respuesta que permite al iniciador derivar una clave de cifrado para las comunicaciones posteriores entre el iniciador y el respondedor [0007].

3.9. El Examinador indica que las reivindicaciones 1 a 5 no definen una invención novedosa a la luz del documento D1. Para esto, el Examinador se refiere a los párrafos [0105], [0104], [0058], [0055], [0104], [0058], [0105], [0058], [0059], [0102], [0105], y [0059] en ese orden, en un intento de tratar de construir desde D1 una descripción que no existe.

3.10. Como bien lo indica el párrafo [0105] de D1 citado por el Examinador: ***“Una vez que esta información se envía al servidor de registro, el servidor de registro puede almacenar y calcular los valores hash necesarios para implementar los registros descritos en este documento y almacenar esas entradas de registro en el almacenamiento de datos, como el almacenamiento de datos (760). Estas entradas de registro pueden contener información sobre la computadora, actividades de la red, transacciones financieras o cualquier otro evento electrónico”***, es claro que el sistema reclamado en D1 procesa y calcula hashes y procesa los datos para la auditoría después de que la transacción ocurre en un servidor o sistema separado y se envía al servidor de registro. El hash no es contemporáneo de la transacción; no se calcula en el mismo flujo de procesamiento de mensajes que la transacción en sí, sino en un sistema separado después del evento.

3.11. A continuación, el examinador se refiere al párrafo [0104]. Sin embargo, ese párrafo también distingue claramente la reivindicación 1 de la presente invención del sistema reivindicado en D1. La segunda oración en el párrafo [0104] simplemente confirma que el sistema en D1 debe realizar una transacción antes de que pueda procesar un hash: ***“El servidor de registro puede recibir mensajes de dispositivos informáticos, como el dispositivo informático 752. Estos mensajes de registro pueden generarse en función de una variedad de eventos y objetos, por ejemplo, actividades de la red informática, transacciones financieras y otros eventos.”***

3.12. El Examinador se refirió a estos dos párrafos anteriormente mencionados en ese orden para objetar la novedad de la reivindicación 1. Sin embargo, al leer los párrafos completos en su orden completo, [0104] y luego [0105], D1 claramente describe un sistema en el que un servidor de registros debe recibir primero una transacción o un mensaje antes de poder procesar el hash. En ninguna parte de la reivindicación 1 se reclama un sistema que primero debe recibir una transacción o mensaje antes de que pueda generar un hash o auditoría de esa transacción o mensaje.

3.13. A continuación, el examinador cita selectivamente el párrafo [0055] antes de volver a referirse al [0104]. Todo lo que revela el [0055] es que el sistema reivindicado en D1 primero esperará recibir un mensaje antes de hacer algo: *“En el bloque 106, se puede recibir un nuevo mensaje de registro o evento para registrar. ... **Dicha información recibida que es un evento puede incluir el mensaje de registro que debe registrarse, o un objeto en un tipo de evento que luego puede generar un mensaje de registro por parte del servidor de registro ...**”*

3.14. En otras palabras, el sistema de D1 solo puede procesar eventos o transacciones después de que el evento haya ocurrido, algo que se confirma leyendo los párrafos [0055], [0104] y [0105] en el orden correcto.

3.15. Luego en su análisis, el Examinador se refiere a se refiere al párrafo [0058]. Sin embargo, este párrafo describe el método en D1 que se basa en un segundo hash de resumen que el sistema reclamado debe almacenar junto con el primer hash, como claramente se indica al principio del párrafo: *“En el bloque 110, después de determinar un hash que depende tanto de la sal como del mensaje de registro actual, que se ingresará en el registro, **se puede calcular un segundo hash, denominado hash de resumen**”.*

3.16. En D1, este hash conduce directamente desde el primer hash para ese mismo evento de registro, el *“hash de registro actual”* como se describe en [0057] y se almacena en la entrada junto con el primer hash [0059]. El párrafo [0058] no divulga *“los primeros datos iniciales”* o los *“segundos datos iniciales”* como afirma el Examinador.

3.17. El párrafo [0059] describe efectivamente cómo el sistema en D1 construye bloques de múltiples entradas de registro antes de que se comprometan con el registro: *“Por ejemplo, si no se va a realizar ningún compromiso en 116, entonces en el bloque 120 el ciclo se repite y el servidor recibe otro mensaje de registro para registrarlo ... este proceso continúa hasta que el servidor/programa de registro decide realizar un nuevo compromiso según lo determinado en el bloque 116”.*

3.18. Esto es lo opuesto al sistema reivindicado en la presente solicitud. Como se mencionó anteriormente, la invención reclamada procesa una transacción y genera y graba el registro o auditoría de esa transacción al mismo tiempo en el mismo proceso.

3.19. Los párrafos [0055] a [0059], cuando se leen juntos en su orden natural, describen un sistema que primero calcula un hash, el hash de registro actual, una vez que ese evento de registro ha ocurrido y se ha pasado al servidor de registro [0055], [0104] y [0105]. Los bloques 106, 108, 110, 112 y 116 en la figura 1 confirman que el sistema en D1 procesa los hash después del evento. Asimismo, el párrafo [0005] describe un sistema informático de registro que: *“puede comprender uno o más procesadores de hardware **configurados para hacer que el sistema informático reciba un evento de una entidad de envío de eventos, comprendiendo el evento los datos del evento que describen el evento, determinar uno o más elementos de metadatos asociados con el evento, calcular un hash de entrada de registro asociado con el evento, ... calcula un hash de resumen de registro asociado con el evento ...**”*.

3.20. El párrafo [0102] establece que el sistema reivindicado en D1 puede utilizar uno o más registros. No se comprende la relevancia de ese párrafo para las reivindicaciones de la presente solicitud, ya que los registros en D1 no son contemporáneos a las transacciones como ampliamente se describe en los párrafos [0055] a [0059] y [0104] a [0105].

3.21. En cuanto al párrafo [0109], al que se refiere el Examinador, se desea resaltar que simplemente confirma que las fuentes de datos a las que se hace referencia en las reivindicaciones de D1, de las que se toman los registros o eventos que se van a extraer pueden adoptar la forma de: *“Unidades de disco duro, memorias de estado sólido y / o cualquier otro tipo de medio de almacenamiento no transitorio, legible por computadora, accesible de forma remota o local para el servidor de aplicaciones 758”*.

3.22. La divulgación en el párrafo [0109] simplemente establece que los datos antes de que se aprueben o después de que se aprueben (ver, por ejemplo, las divulgaciones en el párrafo [0105]) se almacenan en un dispositivo informático, distinguiendo aún más nuestras reivindicaciones de las de D1. Como se señaló anteriormente, en ninguna parte de la descripción o de las reivindicaciones, se reclama un sistema que primero debe almacenar una transacción antes de que el sistema pueda procesar esa transacción. El sistema, en cambio, elimina esa brecha de tiempo, a diferencia del de D1.

3.23. Por todo lo anteriormente descrito, se debe tener en cuenta que la reivindicación 1 si cuenta con novedad frente a las enseñanzas de D1.

3.24. En cuanto a la novedad de las reivindicaciones 2 a 5, el Solicitante respetuosamente se encuentra en desacuerdo con la conclusión de que el documento D1 citado divulga las características de la reivindicación dependiente 2 o la reivindicación 3. Como se mencionó anteriormente, los párrafos [0058] a [0059] de D1 divulgan un sistema en el que eso genera un hash de un evento, incluyendo una marca de tiempo, después de que el sistema registra o genera ese evento. Esto es válido también para el párrafo [0053] en D1, que, como confirman los párrafos [0058] a [0059], se refiere a valores hash que se generan después de que se registra un evento. El párrafo [0105] confirma esto al comienzo del párrafo, como se indicó en los comentarios de la novedad de la reivindicación 1.

3.25. Asimismo, el Solicitante no se encuentra de acuerdo con el Examinador en que el párrafo [0053] en D1 divulga la materia de las reivindicaciones 4 o 5. El párrafo [0053], cuando se lee con [0058] a [0059] describe cómo el sistema reivindicado en D1 crea una cadena de hashes después del evento, que luego bloquea todas las entradas anteriores en una cadena irrevocable. La primera parte de ese párrafo es importante ya que revela que el sistema requiere dos entradas para firmar y marcar la hora (sic) en la cadena: ***“Después del inicio de la cadena, puede ocurrir una segunda entrada de registro que firma y marca la hora de la cadena. Por ejemplo, en el bloque 104, se puede crear una segunda entrada de registro correspondiente a una entrada de confirmación que bloquea todas las entradas anteriores del registro”***.

3.26. Esto no es lo que se reclama en las reivindicaciones 4 y 5 de la presente invención, pues el sistema no necesita dos entradas de registro separadas para bloquear todas las entradas anteriores. Los párrafos [0053] a [0059] en D1 describen una versión de Blockchain que procesa, aplica hash y registra transacciones después de que han ocurrido.

3.27. Por su parte, el párrafo [0049] se refiere a las figuras 1 y 2 en D1, que describen en forma gráfica cómo el sistema de D1 inicia una cadena de auditoría después de haber recibido el primer evento de hash. No puede iniciar el proceso al mismo tiempo que el primer evento. Para entender esto, [0049] debe leerse junto con [0048], que establece claramente que: *“La Figura 1 ilustra un flujo de instrucciones de método o programa para un servidor de registro (o servidores) o programa (o programas), que recibe nuevos eventos o entradas de registro para ser incluidos en el registro, como el servidor que se muestra en la Figura 7”*.

3.28. El párrafo [0049] continúa diciendo inmediatamente: *“En el bloque 102, se puede iniciar un nuevo registro a través de una entrada de registro inicial ... Además, puede comprender un hash de registro que se calcula sobre el mensaje, y es dependiente de, el mensaje vacío / firma digital y una sal aleatoria. También puede comprender un valor hash de resumen. El valor de*

*resumen de hash puede depender del hash de registro original para el mensaje vacío y varios metadatos para el mensaje vacío. **Dicho hash de resumen** puede considerarse el inicio de la cadena de hash que se puede utilizar para verificar los mensajes de registro posteriores.”*

3.29. El texto al que se refiere el Examinador no se puede leer de forma aislada. Cuando se lee con el párrafo [0048], continúa y se encuentra con los párrafos [0053] a [0059], a los que nos hemos referido anteriormente. Estos, cuando se leen juntos, confirman que los hash a los que se hace referencia en los párrafos [0048] a [0059] ocurren después de que se ha registrado un evento, incluso el hash utilizado para iniciar una cadena de auditoría. No ocurren ni pueden ocurrir al mismo tiempo que los eventos mismos. No hacen nada para eliminar el lapso de tiempo entre una transacción y la auditoría de esa transacción. El párrafo [0074] revela que: *"La entrada de registro 302, al igual que otras entradas de registro en esta divulgación, puede incluir el hash de registro 1, que se puede calcular sobre el mensaje de registro, como la firma digital con marca de tiempo sobre el hash de resumen 0, y una sal que proporciona aleatorización".*

3.30. Esto resume las divulgaciones en los párrafos [0048] a [0059] para confirmar que el sistema de D1 crea registros o auditorías después del evento. Sin embargo, está más restringido ya que se refiere específicamente a la figura 3, que es un ejemplo de un registro redactado, un extracto de un registro existente, como lo confirma el texto del párrafo [0073]: ***"La Fig. 3 ilustra una realización de muestra de un segmento de registro redactado. En algunas realizaciones, el segmento de ejemplo que aparece en la FIG. 3 puede comenzar con una entrada de registro con una firma digital de marca de tiempo... "***

3.31. De nuevo, al igual que con las otras reivindicaciones en D1, nada en los párrafos [0073] a [0074] describe un método para procesar y auditar una transacción al mismo tiempo. Todas las auditorías son posteriores al evento.

3.32. Al citar selectivamente los párrafos [0049] y [0074], el Examinador ha intentado construir una divulgación que no existe. Los párrafos [0033] a [0034], [0048] a [0049], [0053] a [0061] y [0073] en D1 describen cómo el sistema reivindicado en ese documento intenta hacer que los registros sean inmutables. El documento describe en los párrafos [0038] a [0040] un método para permitir que un sistema extraiga y vea registros redactados mientras retiene los registros originales en su lugar en un estado inalterado. El párrafo [0040], por ejemplo, describe un método para minimizar las circunstancias en las que una redacción: *"... puede no ser 100% efectiva, especialmente cuando un atacante puede generar entradas de registro candidatas en función de los valores hash asociados en el registro ...".*

3.33. La redacción y la eliminación son actividades independientes. La presentación de registros redactados no elimina ni destruye el original. D1 simplemente describe un método para presentar un subconjunto del registro original donde una o más entradas en ese subconjunto han sido redactadas y donde permanecen, como deben, en el registro original. D1 no revela, como sí se hace en la descripción de la presente solicitud, un método para enmendar la auditoría original para enmendar o destruir un registro, como cuando un tribunal u organismo regulador u obligación ordena la destrucción o enmienda de ese registro. El sistema en D1 no puede hacer esto ya que ha seguido la ruta dictada por la técnica anterior para intentar evitar cualquier cambio en los registros de auditoría.

3.34. Por lo tanto, se debe tener en cuenta que las reivindicaciones 2 a 5 no se encuentran reveladas por D1, por lo tanto, si cumplen el requisito de novedad.

3.35. Ahora, el Examinador en su análisis, también indica que las reivindicaciones 6 a 10 serían obvias para una persona versada en la materia a la luz de las enseñanzas de D1 y D2. El Solicitante respetuosamente se encuentra en desacuerdo.

3.36. Las reivindicaciones y divulgaciones en el documento D1, y de hecho todos los desarrollos en torno a Blockchain y los sistemas similares a Blockchain, se han concentrado en tratar de evitar cualquier alteración del Blockchain o crear nuevos usos para ese sistema. Esa es la dirección en la que el estado de la técnica ha llevado a los expertos en la materia. Ninguno ha intentado eliminar la brecha temporal entre la transacción o evento y su auditoría; se pensaba que era una tarea imposible hasta ahora. Las jurisdicciones han creado reglas legales y reglamentarias para lidiar con la evidencia y los registros informáticos debido a esa brecha temporal (en las jurisdicciones de derecho anglosajón, los registros informáticos y las pistas de auditoría son pruebas que no son tenidas en cuenta (hearsay evidence), mientras que, en las jurisdicciones de derecho civil, los tribunales dan menos importancia a esos registros que a las pruebas contemporáneas). Las empresas gastan pequeñas fortunas tratando de demostrar que las transacciones que se utilizaron para generar hashes no se interfirieron antes de que se generaran esos hashes debido al efecto de esas reglas.

3.37. El examinador afirma que el problema técnico objetivo que la invención en las reivindicaciones 6 a 10 busca resolver se puede formular como: *"Cómo modificar el método conocido en D1 para autenticar cada uno de los pasos de la transacción de datos usando criptografía"*.

3.38. El Solicitante se encuentra en desacuerdo. La invención, como se discutió anteriormente, es resolver el problema técnico de cómo procesar una transacción y la auditoría de esa transacción simultáneamente en el mismo flujo de procesamiento de mensajes para eliminar el lapso de tiempo entre una transacción y su auditoría. No es utilizar ni modificar el método conocido en D1 ya que eso impediría lograr el objetivo de la presente invención. Las divulgaciones en D1 y D2 no mencionan nada similar al respecto.

3.39. El documento D2 simplemente describe un método para establecer comunicaciones seguras entre dos dispositivos mediante el uso de un sistema de clave pública o el uso de un algoritmo J-Pake. No hace nada más. Los pasos que D2 revela en los párrafos [0144] a [0156] no son más que una reformulación de la descripción del funcionamiento del algoritmo J-PAKE y una prueba de conocimiento cero asociada cuando se utilizan para establecer una clave de sesión como se indica en la descripción en uno de los dos primeros borradores iniciales de su especificación (ver [draft-hao-jpake-00 \(ietf.org\)](#) y [draft-hao-jpake-01 \(ietf.org\)](#)). Las versiones provisionales restantes de la descripción y el borrador final se publicaron después de la fecha del D2). Por ejemplo, los campos "g" a los que se refiere D2 son simplemente los generadores numéricos utilizados para calcular las claves de sesión eventuales. Estos generadores son creados por J-PAKE y algoritmos de prueba de conocimiento cero. Los campos zkp simplemente almacenan las exponenciales a las que se elevan los generadores. La presente invención no reclama dichos campos, ni los demás definidos por el estándar, ya que esto equivaldría a intentar reclamar una patente para un algoritmo: ninguno es relevante para las reclamaciones de la presente invención; simplemente se utilizan en J-PAKE y en algoritmos de prueba de conocimiento cero para crear una clave de sesión que actúa como clave criptográfica para cifrar las comunicaciones en D2. Se puede utilizar un método similar para establecer comunicaciones en el sistema reivindicado. Sin embargo, eso no es lo que se está reclamando, ya que se divulgaron en el borrador original del estándar J-PAKE. El documento D2 analiza cómo se puede usar J-PAKE para generar una clave de sesión que dos dispositivos pueden usar para establecer comunicaciones seguras. Pero eso no es lo que se afirma en las reivindicaciones 6 a 10, ni tampoco en ninguna parte de la descripción o reivindicaciones.

3.40. El Examinador correctamente afirma que: *“es conocido en el estado de la técnica el uso del protocolo de prueba de conocimiento cero para métodos criptográficos”*.

3.41. Si bien el Solicitante no discute con esa afirmación, de nuevo argumenta que eso no es lo que pretende con su invención. No reclama el uso de una prueba de conocimiento cero para

generar una clave de sesión para proporcionar una clave criptográfica para comunicaciones seguras.

3.42. Las reivindicaciones 6 a 10 no son para un mecanismo de intercambio de claves, clave pública o de otro tipo, y en ninguna parte mencionan ese uso. Las reivindicaciones 6 a 10 son para un método de utilizar una prueba de conocimiento cero para procesar el hash de auditoría y la transacción simultáneamente en el mismo flujo de procesamiento de mensajes y así eliminar la brecha temporal entre una transacción o evento y la auditoría de ese evento. De hecho, las reivindicaciones van más allá y permiten que el sistema procese cada paso de una transacción al mismo tiempo que la auditoría de ese paso. En las reivindicaciones 2 a 10, no es necesario registrar una transacción o evento antes de que el sistema genere el hash. Las reivindicaciones 6 a 10 se refieren a métodos que utilizan una prueba de conocimiento cero, no a un algoritmo de intercambio de claves.

3.43. Las reivindicaciones 6-10 van más allá del progreso normal de la tecnología; no reclaman un algoritmo de intercambio de claves como se usa en la técnica anterior para intercambiar una clave de sesión que luego se usa para cifrar las comunicaciones. Afirman algo más allá del progreso normal de la tecnología, que consiste en utilizar una prueba de conocimiento cero, independientemente de cómo se implemente, para procesar el hash de auditoría y la transacción simultáneamente en el mismo flujo de procesamiento de mensajes para eliminar la brecha temporal entre una transacción o evento y la auditoría de ese evento. El estado de la técnica no menciona tal uso y no se puede inferir ninguno. De hecho, el Solicitante sostiene que el estado de la técnica aleja al experto en la materia del procedimiento propuesto por la invención.

3.44. Si, como afirma el Examinador, D2 revela el material de la invención en cuestión, entonces D2 reclamaría un método para utilizar una prueba de conocimiento cero para eliminar la brecha temporal entre una transacción y la auditoría de esa transacción. Pero D2 no lo hace. Como se indicó anteriormente, las divulgaciones en D2 describen efectivamente cómo funciona J-PAKE. En ninguna parte contiene la idea de que una prueba de conocimiento cero se puede usar para procesar una transacción y la auditoría de esa transacción simultáneamente en el mismo flujo de procesamiento de mensajes, de modo que eliminemos el lapso de tiempo entre una transacción y su auditoría.

3.45. Si, como afirma el Examinador las reivindicaciones 6 a 10 fueran obvias para una persona experta en la técnica anterior, los incentivos económicos para eliminar la brecha temporal habrían resultado en un sistema que lo hizo. Hasta la fecha, no existe tal sistema que no sea el que el Solicitante reclama. Si fuera obvio, se habría esperado que un solicitante del calibre del de D2

hubiera hecho la afirmación. Pero no lo hicieron. De hecho, la discusión en [0144] a [0156] en D2 pierde completamente la capacidad de usar el J-PAKE, o de hecho cualquier otro algoritmo PAKE, y una prueba de conocimiento cero, asociada de una manera que permite a alguien procesar una transacción y auditar esa transacción de la misma manera. Pasa por alto por completo el hecho de que el algoritmo J-PAKE puede utilizarse para comunicaciones muy seguras y hacer uso de una infraestructura de clave pública en lugar de utilizar contraseñas compartidas de entropía relativamente baja [0138]. En cambio, D2 simplemente sigue el camino dictado por la técnica anterior.

3.46. Por lo tanto, el Solicitante sostiene que el mismo hecho de que D2 no mencione ningún uso de J-PAKE o la prueba de conocimiento cero para procesar una transacción y la auditoría de esa transacción simultáneamente en el mismo flujo de procesamiento de mensajes para eliminar la brecha de tiempo entre una transacción y su auditoría, solo confirma el nivel inventivo que tiene la invención en cuestión frente al estado de la técnica existente.

3.47. Por todo lo anteriormente expuesto, se solicita que se den por superadas las objeciones a la solicitud de patente, teniendo en cuenta que la invención sí cumple con los requisitos de novedad y nivel inventivo.

4. PETICIÓN

Teniendo en cuenta que se ha dado respuesta a todas las observaciones realizadas por su Despacho, demostrando que el pliego reivindicatorio es claro y cumple con los requisitos de patentabilidad, amablemente se solicita proceder al otorgamiento de la solicitud de patente.

5. NOTIFICACIONES

Recibiré notificaciones en la secretaría de su Despacho; en mis oficinas de abogado ubicadas en la Calle 67 No. 7 – 35, oficina 1204, teléfono 3192900, fax 3210295, Bogotá D.C., Colombia, o; al correo electrónico patentes@gomezpinzon.com.

Atentamente,

MAURICIO JARAMILLO C.

C.C. 80.421.942 de Bogotá

T.P. 74.555 del C.S.J.

cmr