

REIVINDICACIONES

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

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

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

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

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

donde el hash biométrico es un hash de datos biométricos del individuo,

y

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

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

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

y

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

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

firmes, utilizando la clave privada a partir de la cual se derivó la dirección de verificación, la verificación de la identidad del individuo como respuesta a la determinación de que el identificador de la petición y los datos biométricos de la petición coinciden con el identificador almacenado y el hash biométrico almacenado.

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

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

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

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

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

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

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

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

almacene, en uno o varios medios de almacenamiento legibles por una computadora, otro hash biométrico del individuo en asociación con la otra dirección de verificación asociada con la cadena de bloques,

donde el otro hash biométrico es un hash de otros datos biométricos del individuo;

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

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

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

6. El sistema de acuerdo con la reivindicación 5, en el cual se hace que el sistema informático del lado del servidor: obtenga, a través de una interfaz de usuario, un comando iniciado por el usuario para añadir la otra dirección de verificación como una dirección de la cadena de bloques para el individuo; y

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

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

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

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

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

proporcione a un primer usuario, que no es el individuo, acceso a los datos almacenados en uno o varios medios de almacenamiento

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

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

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

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

11. Un método para proporcionar una verificación de la identidad personal multifactorial basada en una cadena de bloques, implementándose el método mediante un sistema informático del lado del servidor que comprende uno o varios procesadores que ejecutan instrucciones de un programa informático que, cuando se ejecutan, llevan a cabo el método, comprendiendo el método:

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

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

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

de bloques,

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

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

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

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

12. El método de acuerdo con la reivindicación 11, que comprende:

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

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

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

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

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

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

14. El método de acuerdo con la reivindicación 11, que comprende:

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

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

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

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

la firma, por el sistema informático del lado del servidor, de la verificación de la identidad del individuo como respuesta a una determinación en cuanto a que el identificador de la petición, los datos biométricos de la petición, los otros datos biométricos de la petición

coinciden con el identificador almacenado, con el hash biométrico almacenado, y con el otro hash biométrico almacenado.

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

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

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

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

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

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

17. El método de acuerdo con la reivindicación 11, que comprende:

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

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

tiene una segunda clave privada.

18. El método de acuerdo con la reivindicación 11, en el cual los datos biométricos comprenden una imagen, un registro o un patrón.

19. El método de acuerdo con la reivindicación 11, en el cual los datos biométricos están relacionados con una huella digital, venas palmares, reconocimiento facial, ADN, huella palmar, geometría de la mano, reconocimiento del iris, retina, olor, andares, o con la voz.

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

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

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

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

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

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

donde cada uno de los siguientes: el identificador, el primer hash

biométrico, el segundo hash biométrico, la primera dirección de verificación y la segunda dirección de verificación son diferentes entre sí, son diferentes de las primeras claves privadas y públicas de las cuales se derivó la primera dirección de verificación, y son diferentes de las segundas claves privadas y públicas de las cuales se derivó la segunda dirección de verificación;

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

obtenga (i) el identificador almacenado y el primer hash biométrico almacenado utilizando la primera dirección de verificación indicada en la petición y (ii) el segundo hash biométrico almacenado utilizando la segunda dirección de verificación indicada en la petición; y

firmes, utilizando la clave privada de la cual se derivó la primera dirección de verificación, la verificación de la identidad del individuo como respuesta a una determinación en cuanto a que el identificador de la petición, los primeros datos biométricos de la petición, y los segundos datos biométricos de la petición coinciden con el identificador almacenado, el primer hash biométrico almacenado y el segundo hash biométrico almacenado;

proporcione a un primer usuario, que no es el individuo, acceso a los datos almacenados en uno o varios medios de almacenamiento legibles por una computadora en asociación con la primera dirección de verificación asociada con la cadena de bloques, donde se le proporciona acceso al primer usuario a los datos almacenados basándose en la verificación de que el primer usuario tiene una primera clave privada, siendo diferente la primera clave privada de la clave privada de la cual se derivó la primera dirección de verificación y siendo diferente de la clave privada de la cual se derivó la segunda dirección de verificación; y

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