



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

909 7590 04/18/2018
Pillsbury Winthrop Shaw Pittman, LLP
PO Box 10500
McLean, VIRGINIA 22102
UNITED STATES OF AMERICA

EXAMINER

GOODCHILD, WILLIAM J

ART UNIT

PAPER NUMBER

2433

DATE MAILED: 04/18/2018

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/083,241	03/28/2016	Marcus Andrade	038918-0444639	5060

TITLE OF INVENTION: SYSTEMS AND METHODS FOR PROVIDING BLOCK CHAIN-BASED MULTIFACTOR PERSONAL IDENTITY VERIFICATION

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	\$500	\$0.00	\$0.00	\$500	07/18/2018

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: **Mail** **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

909 7590 04/18/2018
Pillsbury Winthrop Shaw Pittman, LLP
PO Box 10500
McLean, VIRGINIA 22102
UNITED STATES OF AMERICA

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/083,241	03/28/2016	Marcus Andrade	038918-0444639	5060

TITLE OF INVENTION: SYSTEMS AND METHODS FOR PROVIDING BLOCK CHAIN-BASED MULTIFACTOR PERSONAL IDENTITY VERIFICATION

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	\$500	\$0.00	\$0.00	\$500	07/18/2018

EXAMINER	ART UNIT	CLASS-SUBCLASS
GOODCHILD, WILLIAM J	2433	726-006000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____
2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☐ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:

4b. Payment of Fee(s): (**Please first reapply any previously paid issue fee shown above**)

☐ Issue Fee

☐ Publication Fee (No small entity discount permitted)

☐ Advance Order - # of Copies _____

☐ A check is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☐ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

☐ Applicant certifying micro entity status. See 37 CFR 1.29

☐ Applicant asserting small entity status. See 37 CFR 1.27

☐ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____

Date _____

Typed or printed name _____

Registration No. _____



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/083,241	03/28/2016	Marcus Andrade	038918-0444639	5060
909	7590	04/18/2018	EXAMINER	
Pillsbury Winthrop Shaw Pittman, LLP			GOODCHILD, WILLIAM J	
PO Box 10500			ART UNIT	
McLean, VIRGINIA 22102			PAPER NUMBER	
UNITED STATES OF AMERICA			2433	

DATE MAILED: 04/18/2018

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b) (Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

<i>Notice Requiring Inventor's Oath or Declaration</i>	Application No. 15/083,241	Applicant(s) Marcus Andrade	
	Examiner GOODCHILD, WILLIAM J	Art Unit 2433	

This notice is an attachment to the Notice of Allowability (PTOL-37), or the Notice of Allowability For A Design Application (PTOL-37D).

An inventor's oath or declaration in compliance with 37 CFR 1.63 or 1.64 executed by or with respect to each inventor has not yet been submitted.

An oath or declaration in compliance with 37 CFR 1.63, or a substitute statement in compliance with 37 CFR 1.64, executed by or with respect to each inventor (for any inventor for which a compliant oath, declaration, or substitute statement has not yet been submitted) **MUST** be filed no later than the date on which the issue fee is paid. See 35 U.S.C. 115(f). Failure to timely comply will result in ABANDONMENT of this application.

A properly executed inventor's oath to declaration has not been received for the following inventor(s):

If applicant previously filed one or more oaths, declarations, or substitute statements, applicant may have received an informational notice regarding deficiencies therein.

The following deficiencies are noted:

INFORMAL ACTION PROBLEMS

- A properly executed inventor's oath or declaration has not been received for the following inventor(s): **Marcus Andrade**.

Applicant may submit the inventor's oath or declaration at any time before the Notice of Allowance and Fee(s) Due, PTOL-85, is mailed.

Questions relating to this Notice should be directed to the Application Assistance Unit at 571-272-4200.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 15/083,241	Applicant(s) Andrade, Marcus	
	Examiner WILLIAM J GOODCHILD	Art Unit 2433	AIA Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 12/19/2017.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3. ☒ The allowed claim(s) is/are 21-40. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a) ☐ All b) ☐ Some *c) ☐ None of the:

1. ☐ Certified copies of the priority documents have been received.

2. ☐ Certified copies of the priority documents have been received in Application No. _____.

3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892) 2. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____. 3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____. 4. ☐ Interview Summary (PTO-413), Paper No./Mail Date. _____.	5. ☐ Examiner's Amendment/Comment 6. ☒ Examiner's Statement of Reasons for Allowance 7. ☐ Other _____.
---	--

/William J. Goodchild/
Primary Examiner, Art Unit 2433

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

Response to Arguments

2. Applicant's arguments, see Remarks, filed 12/19/2017, with respect to claims 21-40 have been fully considered and are persuasive. The 102/103 rejections have been withdrawn.

Allowable Subject Matter

3. Claims 21-40 are allowed.

4. The following is an examiner's statement of reasons for allowance: amended independent claims relating to "wherein each of the identifier, the biometric hash, and the verification address are different from one another and different from private and public keys from which the verification address was derived;" and "obtain, from a client-side device, the identifier and the biometric data in connection with a request to verify the individual's identity, the request indicating the verification address of the blockchain" are not found within the art of record.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably

accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to WILLIAM J GOODCHILD whose telephone number is (571)270-1589. The examiner can normally be reached on M-F 8am-4:30pm.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at <http://www.uspto.gov/interviewpractice>.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jeff Pwu can be reached on 571-272-6798. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

Application/Control Number: 15/083,241
Art Unit: 2433

Page 4

USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/William J. Goodchild/
Primary Examiner, Art Unit 2433

This listing of claims will replace all prior versions and listings of claims in the Application.

LISTING OF CLAIMS:

1-20. (Cancelled)

21. (New) A system for providing blockchain-based multifactor personal identity verification, the system comprising:

one or more computer-readable storage media configured to store a blockchain;

a server-side computer system comprising one or more processors programmed to execute computer program instructions that, when executed, cause the server-side computer system to:

assign a verification address associated with the blockchain to an individual, the individual having a previously verified personal identity;

store, at the one or more computer-readable storage media, an identifier of the individual and a biometric hash of the individual in association with the verification address associated with the blockchain,

wherein the biometric hash is a hash of biometric data of the individual,
and

wherein each of the identifier, the biometric hash, and the verification address are different from one another and different from private and public keys from which the verification address was derived;

obtain, from a client-side device, the identifier and the biometric data in connection with a request to verify the individual's identity, the request indicating the verification address associated with the blockchain;

obtain the stored identifier and the stored biometric hash using the verification address indicated in the request; and

sign verification of the individual's identity responsive to a determination that the identifier of the request and the biometric data of the request match the stored identifier and the stored biometric hash.

22. (New) The system of claim 21, wherein the server-side computer system is caused to:
sign, using the private key from which the verification address was derived, the verification of the individual's identity responsive to the determination that the identifier of the request and the biometric data of the request match the stored identifier and the stored biometric hash.
23. (New) The system of claim 22, wherein the server -side computer system is caused to:
store, at the one or more computer-readable storage media, the private key in association with the verification address associated with the blockchain;
obtain, from the client-side device, the private key in connection with the request to verify the individual's identity;
obtain the stored private key using the verification address indicated in the request; and
sign, using the private key, the verification of the individual's identity responsive to a determination that the identifier of the request, the biometric data of the request, and the private key of the request match the stored identifier, the stored biometric hash, and the stored private key.
24. (New) The system of claim 23, wherein the private key is also stored on the client-side device, and wherein the client-side device is a user device of the individual.
25. (New) The system of claim 21, wherein the server-side computer system is caused to:
assign another verification address associated with the blockchain to the individual;
store, at the one or more computer-readable storage media, another biometric hash of the individual in association with the other verification address associated with the blockchain, the other biometric hash being a hash of other biometric data of the individual;
obtain, from the client-side device, the other biometric data in connection with the request to verify the individual's identity, the request further indicating the other verification address associated with the blockchain;
obtain the stored other biometric hash using the other verification address indicated in the request; and

sign the verification of the individual's identity responsive to a determination that the identifier of the request, the biometric data of the request, the other biometric data of the request match the stored identifier, the stored biometric hash, and the stored other biometric hash.

26. (New) The system of claim 25, wherein the server-side computer system is caused to:
obtain, via a user interface, a user-initiated command to add the other verification address as an address of the blockchain for the individual; and
assign the other verification address associated with the blockchain to the individual based on the user-initiated command.

27. (New) The system of claim 25, wherein the server-side computer system is caused to:
obtain, via a user interface, a user-initiated command to remove the other verification address as an address of the blockchain for the individual; and
de-associate the other verification address associated with the blockchain from the individual based on the user-initiated command.

28. (New) The system of claim 21, wherein the server-side computer system is caused to:
provide a first user, different than the individual, access to data stored at the one or more computer-readable storage media in association with the verification address associated with the blockchain, the first user being provided access to the stored data based on verification that the first user has a first private key, the first private key being different the private key from which the verification address was derived; and
denying a second user, different than the individual, access to the stored data based on verification that the second user has a second private key.

29. (New) The system of claim 21, wherein the biometric data comprises an image, a recording, or a template.

30. (New) The system of claim 21, wherein the biometric data is related to a fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina, odor, gait, or voice.

31. (New) A method of providing blockchain-based multifactor personal identity verification, the method being implemented by a server-side computer system comprising one or more processors executing computer program instructions that, when executed, perform the method, the method comprising:

storing, by the server-side computer system, a blockchain at one or more computer-readable storage media of the server-side computer system;

assigning, by the server-side computer system, a verification address associated with the blockchain to an individual, the individual having a previously verified personal identity;

storing, by the server-side computer system, at the one or more computer-readable storage media, an identifier of the individual and a biometric hash of the individual in association with the verification address associated with the blockchain,

wherein the biometric hash is a hash of biometric data of the individual, and

wherein each of the identifier, the biometric hash, and the verification address are different from one another and different from private and public keys from which the verification address was derived;

obtaining, by the server-side computer system, from a client-side device, the identifier and the biometric data in connection with a request to verify the individual's identity, the request indicating the verification address associated with the blockchain;

obtaining, by the server-side computer system, the stored identifier and the stored biometric hash using the verification address indicated in the request; and

assigning, by the server-side computer system, verification of the individual's identity responsive to a determination that the identifier of the request and the biometric data of the request match the stored identifier and the stored biometric hash.

32. (New) The method of claim 31, comprising:

signing, by the server-side computer system, using the private key from which the verification address was derived, the verification of the individual's identity responsive to the

determination that the identifier of the request and the biometric data of the request match the stored identifier and the stored biometric hash.

33. (New) The method of claim 32, comprising:

storing, by the server-side computer system, at the one or more computer-readable storage media, the private key in association with the verification address associated with the blockchain;

obtaining, by the server-side computer system, from the client-side device, the private key in connection with the request to verify the individual's identity;

obtaining the stored private key using the verification address indicated in the request; and

signing, by the server-side computer system, using the private key, the verification of the individual's identity responsive to a determination that the identifier of the request, the biometric data of the request, and the private key of the request match the stored identifier, the stored biometric hash, and the stored private key.

34. (New) The method of claim 31, comprising:

assigning, by the server-side computer system, another verification address associated with the blockchain to the individual;

storing, by the server-side computer system, at the one or more computer-readable storage media, another biometric hash of the individual in association with the other verification address associated with the blockchain, the other biometric hash being a hash of other biometric data of the individual;

obtaining, by the server-side computer system, from the client-side device, the other biometric data in connection with the request to verify the individual's identity, the request further indicating the other verification address associated with the blockchain;

obtaining, by the server-side computer system, the stored other biometric hash using the other verification address indicated in the request; and

signing, by the server-side computer system, the verification of the individual's identity responsive to a determination that the identifier of the request, the biometric data of the request, the other biometric data of the request match the stored identifier, the stored biometric hash, and the stored other biometric hash.

35. (New) The method of claim 34, comprising:

obtaining, by the server-side computer system, via a user interface, a user-initiated command to add the other verification address as an address of the blockchain for the individual; and

assigning, by the server-side computer system, the other verification address associated with the blockchain to the individual based on the user-initiated command.

36. (New) The method of claim 34, comprising:

obtaining, by the server-side computer system, via a user interface, a user-initiated command to remove the other verification address as an address of the blockchain for the individual; and

de-associating, by the server-side computer system, the other verification address associated with the blockchain from the individual based on the user-initiated command.

37. (New) The method of claim 31, comprising:

providing, by the server-side computer system, a first user, different than the individual, access to data stored at the one or more computer-readable storage media in association with the verification address associated with the blockchain, the first user being provided access to the stored data based on verification that the first user has a first private key, the first private key being different the private key from which the verification address was derived; and

denying, by the server-side computer system, a second user, different than the individual, access to the stored data based on verification that the second user has a second private key.

38. (New) The method of claim 31, wherein the biometric data comprises an image, a recording, or a template.

39. (New) The method of claim 31, wherein the biometric data is related to a fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina, odor, gait, or voice.

40. (New) A system for providing blockchain-based multifactor personal identity verification, the system comprising:

one or more computer-readable storage media configured to store a blockchain;

a server-side computer system comprising one or more processors programmed to execute computer program instructions that, when executed, cause the server-side computer system to:

assign multiple verification addresses of the blockchain to the individual, the individual having a previously verified personal identity, the multiple verification addresses include a first verification address associated with the blockchain and a second verification address associated with the blockchain;

store, at the one or more computer-readable storage media, (i) an identifier of the individual and a first biometric hash of the individual in association with the first verification address associated with the blockchain and (ii) a second biometric hash of the individual in association with the second verification address associated with the blockchain,

wherein the first biometric hash is a hash of first biometric data of the individual, and the second biometric hash is a hash of second biometric data of the individual, and

wherein each of the identifier, the first biometric hash, the second biometric hash, the first verification address, and the second verification address are different from one another, different from first private and public keys from which the first verification address was derived, and different from second private and public keys from which the second verification address was derived;

obtain, from a client-side device, the identifier, the first biometric data, and the second biometric data in connection with a request to verify the individual's identity, the request indicating the first verification address associated with the blockchain and the second verification address associated with the blockchain;

obtain (i) the stored identifier and the stored first biometric hash using the first verification address indicated in the request and (ii) the stored second biometric hash using the second verification address indicated in the request; and

sign, using the private key from which the first verification address was derived,

verification of the individual's identity responsive to a determination that the identifier of the request, the first biometric data of the request, and the second biometric data of the request match the stored identifier, the stored first biometric hash, and the stored second biometric hash;

provide a first user, different than the individual, access to data stored at the one or more computer-readable storage media in association with the first verification address associated with the blockchain, the first user being provided access to the stored data based on verification that the first user has a first private key, the first private key being different the private key from which the first verification address was derived and different from the private key from which the second verification address was derived; and

deny a second user, different than the individual, access to the stored data based on verification that the second user has a second private key.



OFICINA DE PATENTES Y MARCAS DE ESTADOS UNIDOS

DEPARTAMENTO DE COMERCIO DE ESTADOS UNIDOS
Oficina de Patentes y Marcas de Estados Unidos
Dirección: COMISIONADO DE PATENTES
P.O. Box 1450
Alexandria, Virginia 22313-1450

NOTIFICACIÓN DE CONCESIÓN Y ARANCEL(ES) ADEUDADO(S)

909 7590 18/04/2018
Pillsbury Winthrop Shaw Pittman, LLP PO
Box 10500 McLean, VIRGINIA 22102
UNITED STATES OF AMERICA

GOODCHILD, WILLIAM J

UNIDAD DEL ARTE NÚMERO DE DOCUMENTO
2433

FECHA DE ENVÍO: 18/04/2018

Nº DE SOLICITUD	FECHA DE PRESENTACIÓN	PRIMER INVENTOR NOMBRADO	Nº DE EXP. DEL ABOGADO	Nº DE CONFIRMACIÓN
-----------------	-----------------------	--------------------------	------------------------	--------------------

15/083.241	03/28/2016	Marcus Andrade	038918-0444639	5060
------------	------------	----------------	----------------	------

TÍTULO DE LA INVENCIÓN : SISTEMAS Y MÉTODOS PARA PROPORCIONAR IDENTIDAD PERSONAL MULTIFACTORIAL BASADA EN CADENA DE BLOQUES
VERIFICACIÓN

TIPO DE SOLIC.	ESTADO DE ENTIDAD	ARANCEL DE CONCESIÓN	ARANCEL DE PUBLICACIÓN	ARANCEL DE CONCESIÓN ABONADO	TOTAL ARANCEL(ES) ADEUDADO(S)	FECHA DE VENCIMIENTO
no provisional	PEQUEÑA	\$500	\$0.00	\$0.00	\$500	18/07/2018

LA SOLICITUD IDENTIFICADA ARRIBA SE HA EXAMINADO Y ESTÁ AUTORIZADA PARA CONCEDERSE COMO PATENTE. EL SEGUIMIENTO SOBRE LOS MÉRITOS ESTÁ CERRADO. ESTA NOTIFICACIÓN DE CONCESIÓN NO ES LA CONCESIÓN DE LOS DERECHOS DE LA PATENTE. ESTA SOLICITUD ESTÁ SUJETA AL RETIRO DE EMISIÓN / INICIATIVA DE LA OFICINA O TRAS LA PETICIÓN DEL SOLICITANTE. VÉASE 37 CFR 1.313 Y MPEP 1308. EL ARANCEL DE CONCESIÓN Y DE PUBLICACIÓN (SI SE REQUIEREN) DEBEN ABONARSE DENTRO DE LOS TRES MESES DESDE LA FECHA DE ENVÍO DE ESTA NOTIFICACIÓN O ESTA SOLICITUD SE CONSIDERARÁ ABANDONADA ESTE PERÍODO FIJADO POR LEY NO PUEDE EXTENDERSE. VÉASE 35 U.S.C. 151. EL ARANCEL DE CONCESIÓN ADEUDADO INDICADO ARRIBA NO REFLEJA UN CRÉDITO POR NINGÚN ARANCEL DE CONCESIÓN ABONADO PREVIAMENTE EN ESTA SOLICITUD. SI ANTERIORMENTE SE HA ABONADO UN ARANCEL DE CONCESIÓN EN ESTA SOLICITUD (COMO SE MUESTRA ARRIBA), LA DEVOLUCIÓN DE LA PARTE B DE ESTE FORMULARIO SI CONSIDERARÁ UNA SOLICITUD PARA VOLVER A APLICAR EL ARANCEL DE CONCESIÓN PREVIAMENTE PAGADO AL ARANCEL DE CONCESIÓN ADEUDADO AHORA. CÓMO RESPONDER ESTA NOTIFICACIÓN:

I. Revise el ESTADO DE ENTIDAD que aparece arriba. Si el ESTADO DE ENTIDAD se muestra como PEQUEÑA O MICRO, verifique si aún aplica esa categoría para ese estado de entidad. Si el ESTADO DE ENTIDAD es el mismo que aparece arriba, abone el/los ARANCEL(ES) TOTALES ADEUDADOS que se muestran arriba. Si el ESTADO DE ENTIDAD es distinto a lo que aparece arriba, en la PARTE B - TRANSMISIÓN DE ARANCEL(ES), complete la sección número 5 titulada "Cambio en el Estado de la Entidad (del estado que se indica arriba)". Para los fines de esta notificación, los aranceles de pequeña entidad son 1/2 de la cantidad de los aranceles sin descuento, y los aranceles de micro entidad son de 1/2 de la cantidad de los aranceles de pequeña entidad.

II. La PARTE B - TRANSMISIÓN DE ARANCEL(ES), o su equivalente, debe completarse y devolverse a la Oficina de Patentes y Marcas de Estados Unidos (USPTO) con su ARANCEL DE CONCESIÓN y ARANCEL DE PUBLICACIÓN (si se requiere). Si carga su(s) arancel(es) a su cuenta de depósito, la sección "4b" de la Parte B - Transmisión de Arancel(es) debe completarse y debe presentarse una copia extra de formulario. Si se presenta un equivalente de la Parte B, debe realizarse claramente una solicitud de volver a aplicar el arancel de concesión previamente pagado, y pueden ocurrir demoras en el procesamiento debido a la dificultad de reconocer el documento como un equivalente de la Parte B.

III. Todas las comunicaciones referidas a esta solicitud deben suministrar el número de solicitud. Sírvase dirigir todas las comunicaciones previas a la concesión a Mail Stop ISSUE FEE a menos que se le indique de otro modo. RECORDATORIO IMPORTANTE: La concesión de patentes de utilidad sobre solicitudes presentadas a partir del 12 de diciembre de 1980 puede requerir el pago de aranceles de mantenimiento. Es responsabilidad de quien presenta la patente asegurar el pago oportuno de los aranceles de mantenimiento cuando se venzan.

PARTE B - TRANSMISIÓN DE ARANCEL(ES)

Completar y enviar este formulario, junto con los aranceles aplicables, a: **Correo Mail Stop ISSUE FEE**
Comisionado de Patentes
P.O. Box 1450
Alexandria, Virginia 22313-1450
o **Fax (571)-273-2885**

INSTRUCCIONES: Este formulario debe usarse para transmitir el ARANCEL DE CONCESIÓN y el ARANCEL DE PUBLICACIÓN (si se requiere). Los bloques 1 a 5 deben completarse donde corresponda. Toda correspondencia adicional que incluya aranceles de la Patente, ordenes de anticipo y notificaciones de mantenimiento se enviará a la dirección postal vigente a menos que se corrija abajo o se indique de otro modo en el Bloque 1, mediante (a) especificación de una nueva dirección postal; y/o (b) indicación de una "DIRECCIÓN DE ARANCELES" separada para notificaciones sobre el arancel de mantenimiento.

DIRECCIÓN POSTAL ACTUAL (Nota: Usar el Bloque 1 para cualquier cambio de dirección)

909 7590 18/04/2018
Pillsbury Winthrop Shaw Pittman, LLP PO
Box 10500 McLean, VIRGINIA 22102
UNITED STATES OF AMERICA

Nota: Un certificado de envío postal solo puede usarse para envíos locales de Transmisión de Arancel(es). Este certificado no puede usarse para ningún otro documento adjunto. Cada documento adicional, tal como una cesión o dibujo formal, debe tener su propio certificado de envío o transmisión.

Certificado de Envío Postal o Transmisión
Certifico en este acto que esta Transmisión de Arancel(es) se deposita en el Servicio Postal Norteamericano con franqueo suficiente para envío de primera clase en un sobre dirigido a la dirección Mail Stop ISSUE FEE que antecede, o se transmite por fax a la USPTO al (571) 273-2885, en la fecha indicada más abajo.

(Nombre del Depositante)

(Firma)

(Date)

Nº DE SOLICITUD	FECHA DE PRESENTACIÓN	PRIMER INVENTOR NOMBRADO	Nº DE EXP. DEL ABOGADO	Nº DE CONFIRMACIÓN
15/083.241	28/03/2016	Marcus Andrade	038918-0444639	5060

TÍTULO DE LA INVENCION: SISTEMAS Y MÉTODOS PARA PROPORCIONAR IDENTIDAD PERSONAL MULTIFACTORIAL BASADA EN CADENA DE BLOQUES
VERIFICACIÓN

TIPO DE SOLICITUD	ESTADO DE ENTIDAD	ARANCEL DE CONCESIÓN VENCIDO	ARANCEL DE PUBLICACIÓN VENCIDO	ARANCEL DE CONCESIÓN PAGADO	TOTAL ARANCEL ADEUDADO	FECHA DE VENCIMIENTO
no provisional	PEQUEÑA	\$500	\$0.00	\$0.00	\$500	18/07/2018
EXAMINADOR		UNIDAD DEL ARTE	CLASE - SUB-CLASE			
GOODCHILD, WILLIAM J		2433	726-006000			

1. Cambio de domicilio postal o indicación de "Domicilio de Aranceles" (37 CFR 1.363).
☐ Formulario de Cambio de domicilio postal (o Cambio de Domicilio de Correspondencia PTO/SB/122) adjunto.

☐ Indicación del "Domicilio de Aranceles" (o Form. de Indicación de "Domicilio de Aranceles PTO/SB/47; Rev 03-02 o más reciente) adjunto. Se requiere el uso de un Número de Cliente.

2. Para imprimir en la primera página de la patente, mencionar
(1) Los nombres de hasta 3 apoderados o agentes registrados
O, alternativamente,
(2) El nombre de una sola empresa (que tiene como miembro un apoderado o agente registrado) y los nombres de hasta 2 apoderados o agentes de patentes registrados. Si no se menciona nombre, no se imprimirá ningún nombre.
3. NOMBRE Y DATOS DE RESIDENCIA DEL CESIONARIO A IMPRIMIR EN LA PATENTE (imprimir o escribir a máquina)
SE DEBE OBSERVAR QUE: A menos que se identifique un cesionario más abajo, no aparecerán datos del cesionario en la patente. Si se identifica un cesionario abajo, el documento se ha presentado como registro como se establece en 37 CFR 3.11. La compleción de este formulario NO sustituye la presentación de una cesión.
(A) NOMBRE DEL CESIONARIO
(B) RESIDENCIA: (CIUDAD Y ESTADO O PAÍS)

- Por favor tildar la categoría o las categorías apropiadas del cesionario (no se imprimirá en la patente): ☐ Individuo ☐ Sociedad u otra entidad de grupo privado ☐ Gobierno
- 4a. Se presentará(n) el(los) siguiente(s) aranceles:
☐ Arancel de Concesión
☐ Arancel de Publicación (No se permite descuento de pequeña entidad)
☐ _____ Orden de anticipo - # Copias

4b. Pago de Arancel(es): (Por favor volver a aplicar primero cualquier arancel previamente abonado como se muestra arriba)
☐ Se adjunta cheque.
☐ Pago por tarjeta de crédito. Se adjunta Formulario PTO-2038.
☐ Se autoriza al director a cargar el(los) arancel(es) requerido, cualquier deficiencia o acreditar cualquier pago extra, a la Cuenta de Depósito Número _____ (adjuntar copia extra de este formulario).

5. Cambio en el Estado de Entidad (del estado indicado arriba)
☐ El solicitante certifica estado de micro entidad. Ver 37 CFR 1.29
☐ El solicitante justifica estado de pequeña entidad. Ver 37 CFR 1.27
☐ El solicitante cambia a estado de arancel regular sin descuento.

NOTA: Sin certificación válida del Estado de Micro Entidad (ver forms. PTO/SB/15A y 15B), no se aceptará pago por la suma de micro entidad a riesgo de abandono de la solicitud.

NOTA: Si la solicitud anteriormente fue por un estado de micro entidad, el tildado de este casillero se considerará una notificación de la pérdida de capacidad como estado de micro entidad.

NOTA: El tildado de este casillero se considerará notificación de la capacidad como estado de pequeña o micro entidad, según corresponda.

NOTA: Este formulario debe firmarse de acuerdo con 37 CFR 1.31 y 1.33. Véase 37 CFR 1.4 para conocer los requerimientos de firma y certificaciones.

Firma Autorizada _____ Fecha _____

Nombre a máquina o impreso

Nº de Registro



OFICINA DE PATENTES Y MARCAS DE ESTADOS UNIDOS

DEPARTAMENTO DE COMERCIO DE ESTADOS UNIDOS
Oficina de Patentes y Marcas de Estados Unidos
Domicilio: COMISIONADO DE PATENTES
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Nº DE SOLICITUD	FECHA DE PRESENTACIÓN	PRIMER INVENTOR NOMBRADO	Nº DE EXP. DEL ABOGADO	Nº DE CONFIRMACIÓN
15/083,241	28/03/2016	Marcus Andrade	038918-0444639	
909	7590	18/04/2018	EXAMINADOR	
Pillsbury Winthrop Shaw Pittman, LLP PO Box 10500 McLean, VIRGINIA 22102 UNITED STATES OF AMERICA			GOODCHILD, WILLIAM J	
			UNIDAD DEL ARTE	NÚMERO DE DOCUMENTO
			2433	
FECHA DE ENVÍO: 18/4/2018				

Determinación del Ajuste del Plazo de Patente según 35 U.S.C. 154 (b)
(Solicitudes presentadas a partir del 29 de mayo de 2000, inclusive)

La Oficina ha interrumpido la provisión del cálculo de Ajuste del Plazo de Patentes (por las siglas del inglés: Patent Term Adjustment (PTA)) con la Notificación de Concesión.

La Sección 1(h) (2) de la Ley de Correcciones Técnicas de AIA 35 U.S.C. 154(b) (3) (B) (i) se modificó para eliminar el requerimiento de que la Oficina proporcione una determinación del ajuste del plazo de patente con la notificación de concesión. Véase Revisiones al Ajuste del Plazo de Patentes, 78 Fed. Reg. 19416, 19417 (1 de abril de 2013). Por lo tanto, la Oficina ya no proporciona una determinación del ajuste del plazo de patente inicial con la notificación de concesión. La Oficina continuará suministrando una determinación del ajuste del plazo de patente con la Carta de Notificación de Concesión que se envía al solicitante aproximadamente tres semanas antes de la fecha de concesión de la patente, se incluirá el ajuste del plazo de patente sobre la misma. Cualquier solicitud de reconsideración de la determinación de ajuste del plazo de patente (o la reincorporación del ajuste del plazo de patente) seguirá el proceso definido en 37 CFR 1.705.

Cualquier consulta relacionada con la determinación del Ajuste o de la Extensión del Plazo de Patente debe dirigirse a la Administración Legal de la Oficina de Patentes al (571)-272-7702. Las preguntas relacionadas con los pagos de aranceles de concesión y publicación deben dirigirse al Centro de Atención al Cliente de la Oficina de Publicación de Patentes al 1-(888)-786-0101 o al (571)-272-4200.

*Notificación que requiere
juramento o declaración del
inventor*

Nº DE SOLICITUD 15/083.241	Solicitante(s) Marcus Andrade	
Examinador GOODCHILD, WILLIAM J	Unidad del arte 2433	

Esta notificación es un anexo a la Notificación de Concesión (PTOL-37), o a la Notificación de Concesión para una Solicitud de Diseño (PTOL-37D).

Aún no se ha presentado un juramento o una declaración del inventor, en cumplimiento con lo dispuesto en 37 CFR 1.63 o 1.64 ejecutado por o con respecto a cada inventor.

Un juramento o una declaración en cumplimiento con 37 CFR 1.63, o una declaración sustituta en cumplimiento con 37 CFR 1.64, ejecutados por, o con respecto a, cada inventor (para cualquier inventor para el cual no se haya presentado aún un juramento, una declaración o una declaración sustituta pertinente) DEBE presentarse no después de la fecha en la cual se abona el arancel de concesión. Véase 35 U.S.C. 115(f). La falta de cumplimiento en término generará el ABANDONO de esta solicitud.

No se ha recibido un juramento o una declaración de inventor debidamente ejecutados para el(los) siguiente(s) inventor(es):
Si el solicitante presentó previamente uno o más juramentos, declaraciones o declaraciones sustitutas, el solicitante puede haber recibido una notificación informativa respecto de las deficiencias encontradas:

INFORMAL ACTION PROBLEMS

- No se ha recibido un juramento o una declaración de inventor ejecutados apropiadamente para el(los) siguiente(s) inventor(es): **Marcus Andrade.**
El solicitante puede presentar el juramento o la declaración del inventor en cualquier momento antes del envío de la Notificación de Concesión y el Vencimiento de Cumplimiento y Ejecución, PTOL-85.
Las preguntas relacionadas con esta Notificación deben dirigirse a la Unidad de Asistencia sobre Solicitudes al 571-272-4200.

Notificación de Concesión

Nº DE SOLICITUD	Solicitante(s)	
15/083,241	Andrade, Marcus	
Examinador	Unidad del arte	Estado AIA
WILLIAM J GOODCHILD	2433	Si

- La FECHA DE ENVÍO de esta comunicación aparece en la carátula con la dirección de correspondencia -

Siendo patentables todas las reivindicaciones, la TRAMITACIÓN SOBRE LOS MÉRITOS ESTÁ (O PERMANECE) CERRADA en esta solicitud. Si no se incluye aquí (o se envió anteriormente), una Notificación de concesión (PTOL-85) u otra comunicación apropiada se enviará en su debido momento. ESTA NOTIFICACIÓN DE CONCESIÓN NO ES UNA CONCESIÓN DEL DERECHO DE PATENTES. Esta solicitud está sujeta a que se retire la concesión a iniciativa de la Oficina o a petición del solicitante. Véase 37 CFR 1.313 y MPEP 1308.

1. ☒ Esta comunicación es la respuesta a 19/12/2017.

☐ Una declaración(es)/declaración(es) jurada(s) según 37 CFR 1.130(b) se presentó el _____.
2. ☐ El solicitante realizó una elección en respuesta a un requerimiento de restricción durante una entrevista el _____; el requerimiento de restricción y elección se han incorporado a esta acción.
3. ☒ La(s) reivindicaciones concedidas es/son 21-40 . Como resultado de la(s) reivindicación(es) concedidas, puede ser elegible para el beneficio del programa de Vía Rápida para la Prosecución de Patentes en una oficina de propiedad intelectual participativa para la correspondiente solicitud. Para mayor información, remítase a http://www.uspto.gov/patents/init_events/pph/index.jsp o envíe una consulta a PPHfeedback@uspto.gov.
4. ☐ Se acusa recibo de la reivindicación para una prioridad extranjera según lo dispuesto en 35 U.S.C. § 119(a)-(d) o (f).

Copias certificadas:

a) ☐ TODAS b) ☐ Algunas *c) ☐ Ninguna de:

1. ☐ Copias certificadas de los documentos de prioridad se han recibido
2. ☐ Copias certificadas de los documentos de prioridad se han recibido en la Solicitud N°. _____.
3. ☐ Copias de las copias certificadas de los documentos de prioridad se han recibido en esta solicitud en etapa nacional de la Oficina Internacional (Regla PCT 17.2(a)).
- * Copias certificadas no recibidas: _____ .

El solicitante tiene TRES MESES DESDE LA "FECHA DEL ENVÍO" de esta comunicación para presentar una respuesta que cumple con los requerimientos indicados abajo. La falta de cumplimiento oportuno generará el ABANDONO de esta solicitud.

ESTE PERÍODO DE TRES MESES NO TIENE PRÓRROGA.

5. ☐ Deben presentarse DIBUJOS CORREGIDOS (como "hojas de reemplazo ").

☐ incluyendo los cambios requeridos por la Enmienda/Comentario del Examinador adjunto en la Vista del Documento No./Datos de correo _____.
- Los signos de identificación tales como el número de solicitud (ver 37 CFR 1.84(c)) deben escribirse en los dibujos en el anverso (no en el reverso) de cada hoja. La(s) hoja(s) de reemplazo debe etiquetarse como tales en el encabezado de acuerdo con 37 CFR 1.121(d).
6. ☐ Debe presentarse el DEPÓSITO DE y/o la INFORMACIÓN sobre el depósito de MATERIAL BIOLÓGICO. Observar el comentario del Examinador adjunto respecto del REQUERIMIENTO PARA DEPÓSITO DE MATERIAL BIOLÓGICO.

Anexo(s)

1. ☒ Notificación de Referencias citadas (PTO-892)
2. ☐ Declaraciones de Divulgación de Información (PTO/SB/08),

Nº de Doc./Fecha de envío _____ .
3. ☐ Comentario del Examinador respecto del requerimiento para depósito de material biológico _____.
4. ☐ Resumen de la entrevista (PTO-413),

Nº de Doc./Fecha de envío..
5. ☐ Enmienda/Comentario del Examinador
6. ☐ Declaración del examinador de los motivos de la Concesión
7. ☐ Otros _____ .

/William J. Goodchild/
Examinador Primario, Unidad del arte 2433

ACCIÓN DETALLADA

Notificación de Pre-AIA o Estado AIA

1. La presente solicitud, presentada el, o después del, 16 de marzo de 2013, está sometida a examen según el primer inventor para presentar las disposiciones de la AIA.

Respuesta a los argumentos

2. Los argumentos del solicitante, véase Comentarios, presentados el 19/12/2017, con respecto a las reivindicaciones 21 - 40 se han considerado de manera completa y son persuasivos. Las 102/103 objeciones se han retirado.

Tema susceptible de concesión

3. Se conceden las reivindicaciones 21-40.
4. Lo que sigue es una declaración del examinador de los motivos de concesión: las reivindicaciones independientes modificadas relacionadas con "donde cada uno del identificador, el resumen biométrico y la dirección de verificación son diferentes entre sí y son diferentes de las llaves privadas y públicas de la cual derivó la dirección de verificación;" y "obtener, de un dispositivo del cliente, el los datos del identificador y biométricos en conexión con una solicitud de verificar la identidad del individuo, donde la solicitud indica la dirección de verificación de la cadena de bloqueo" no se encuentran dentro del arte previo. Cualquier comentario considerado necesario de parte del solicitante debe presentarse antes de que se realice el pago del arancel de concesión y, para evitar demoras en el procesamiento, preferentemente debe acompañar el arancel de concesión. Dichas presentaciones deben etiquetarse claramente como "Comentarios sobre la Declaración de los Motivos de Concesión."

Conclusión

5. Cualquier consulta relacionada con esta comunicación o con comunicaciones anteriores del examinador debe dirigirse a WILLIAM J GOODCHILD cuyo número de teléfono es (571)270-1589. El examinador puede contactarse normalmente de L. a V. de 8:00 a 16:30 hs.

Las entrevistas con el Examinador están a disposición por teléfono, en persona y por conferencia en video con el uso de una herramienta de colaboración basada en Internet proporcionada por la USPTO. Para programar una entrevista, se alienta al solicitante a usar la Solicitud de Entrevista Automática de la USPTO (Automated Interview Request (AIR)) en <http://www.uspto.gov/interviewpractice>.

Si los intentos por contactar al examinador son negativos, se puede comunicar con el supervisor del examinador, Jeff Pwu al 571-272-6798. El número de teléfono - fax para la organización donde se asigna esta solicitud o este procedimiento es el 571-273-8300.

La información referida al estado de una solicitud puede obtenerse del sistema de Recuperación de Información de Solicitudes de Patentes (del inglés, Patent Application Information Retrieval (PAIR)). La información sobre el estado para solicitudes publicadas puede obtenerse indistintamente del PAIR privado como del PAIR público. La información sobre el estado de solicitudes no publicadas se encuentra disponible solamente a través del PAI Privado. Para mayor información sobre el sistema PAIR, remítase a <http://pair-direct.uspto.gov>. En el caso de surgir preguntas sobre el acceso al sistema PAIR Privado, comuníquese con el Centro de Comercio Electrónico (EBC) al 866-217-9197 (gratuito). Si necesita asistencia de un

Solicitud/Número de Control: 15/083.241

Página 4

Unidad del arte: 2433

Representante de Atención al Cliente de la USPTO o acceder al sistema de información automática, llame al 800-786-9199 (EN EE. UU. o CANADÁ) o al 571 -272-1000.

/William J. Goodchild/

Examinador Primario, Unidad del arte 2433

Esta lista de reivindicaciones reemplazará a las versiones y listas anteriores en la Solicitud.

LISTING OF CLAIMS:

1-20. (Canceladas)

21. (Nueva) Un sistema para proporcionar verificación de identidad personal multifactorial basada en cadena de bloques, caracterizado porque el sistema comprende:

uno o más medios de almacenamiento legibles por computadora para almacenar una cadena de bloques; un sistema informático instalado en un servidor que comprende uno o más procesadores programados para ejecutar instrucciones del programa informático que, cuando se ejecuta, hace que el sistema informático instalado en el servidor:

asignar una dirección de verificación asociada con la cadena de bloques a un individuo, donde el individuo tiene una identidad personal previamente verificada;

almacenar, en uno o más medios de almacenamiento legibles por computadora, un identificador del individuo y el resumen biométrico del individuo en asociación con la dirección de verificación asociada con la cadena de bloques,

donde el resumen biométrico es un resumen de los datos biométricos del individuo, y

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

obtener, de un dispositivo del cliente, el identificador y los datos biométricos en conexión con una solicitud para verificar la identidad del individuo, donde la solicitud indica la dirección de verificación asociada con la cadena de bloques;

obtener el identificador almacenado y el resumen biométrico almacenado con el uso de la dirección de verificación indicada en la solicitud; y

firmar la verificación de la identidad del individuo en respuesta a una determinación de que el identificador de la solicitud y los datos biométricos de la solicitud coinciden con el identificador almacenado y el resumen biométrico almacenado.

22. (Nueva) El sistema de acuerdo con la reivindicación 21, caracterizado porque se hace que el sistema informático instalado en el servidor: firme, con el uso de la llave privada de cuya dirección de verificación derivó, la verificación de la identidad del individuo en respuesta a la determinación de que el identificador de la solicitud y los datos biométricos de la solicitud coinciden con el identificador almacenado y el resumen biométrico almacenado.
23. (Nueva) El sistema de acuerdo con la reivindicación 22, caracterizado porque se hace que el sistema informático instalado en el servidor: almacene, en uno o más medios de almacenamiento legibles por computadora, la llave privada en asociación con la dirección de verificación asociada con la cadena de bloques; obtener, del dispositivo del cliente, la llave privada en conexión con la solicitud para verificar la identidad del individuo; obtener la llave privada almacenada con el uso de la dirección de verificación indicada en la solicitud; y firmar, con el uso de la llave privada, la verificación de la identidad del individuo en respuesta a una determinación de que el identificador de la solicitud, los datos biométricos de la solicitud, y la llave privada de la solicitud coinciden con el identificador almacenado, el resumen biométrico almacenado y la llave privada almacenada.
24. (Nueva) El sistema de acuerdo con la reivindicación 23, caracterizada porque la llave privada también se almacena en el dispositivo del cliente, y donde el dispositivo del cliente es un dispositivo de usuario del individuo.
25. (Nueva) El sistema de acuerdo con la reivindicación 21, caracterizado porque se hace que el sistema informático instalado en el servidor: asigne otra dirección de verificación asociada con la cadena de bloques del individuo; almacene, en uno o más medios de almacenamiento legibles por computadora, otro resumen biométrico del individuo en asociación con la otra dirección de verificación asociada con la cadena de bloques, donde el otro resumen biométrico es un resumen de otros datos biométricos del individuo; obtener, del dispositivo del cliente, los otros datos biométricos en conexión con la solicitud para verificar la identidad del individuo, donde la solicitud indica, además, la otra dirección de verificación asociada con la cadena de bloques; obtener el otro resumen biométrico almacenado con el uso de la otra dirección de verificación indicada en la solicitud; y

firmar la verificación de la identidad del individuo en respuesta a una determinación de que el identificador de la solicitud, los datos biométricos de la solicitud, y los otros datos biométricos de la solicitud coinciden con el identificador almacenado, el resumen biométrico almacenado y el otro resumen biométrico almacenado.

26. **(Nueva)** El sistema de acuerdo con la reivindicación 25, caracterizado porque se hace que el sistema informático instalado en el servidor : obtenga, a través de una interfaz de usuario, un comando iniciado por el usuario para agregar la otra dirección de verificación como una dirección de la cadena de bloques para el individuo; y
asignar la otra dirección de verificación asociada con la cadena de bloques al individuo en base al comando iniciado por el usuario.

27. **(Nueva)** El sistema de acuerdo con la reivindicación 25, caracterizado porque se hace que el sistema informático instalado en el servidor : obtenga, a través de una interfaz de usuario, un comando iniciado por el usuario para quitar la otra dirección de verificación como una dirección de la cadena de bloques para el individuo; y
desasociar la otra dirección de verificación asociada con la cadena de bloques del individuo en base al comando iniciado por el usuario.

28. **(Nueva)** El sistema de acuerdo con la reivindicación 21, caracterizado porque se hace que el sistema informático instalado en el servidor: proporcione un primer usuario, diferente del individuo, acceda a los datos almacenados en el uno o más
medios de almacenamiento legibles por computadora en asociación con la dirección de verificación asociada con la cadena de bloques, donde al primer usuario se le brinda acceso a los datos almacenados en base a la verificación de que el primer usuario tiene una primera llave privada, donde la primera llave privada es diferente de la llave privada de la cual derivó la dirección de verificación; y

denegar a un segundo usuario, distinto del individuo, acceso a los datos almacenados en base a la verificación de que el segundo usuario tiene una segunda llave privada.

29. **(Nueva)** El sistema de acuerdo con la reivindicación 21, caracterizado porque los datos biométricos comprenden una imagen, una grabación o un patrón.

30. (Nueva) El sistema de acuerdo con la reivindicación 21, caracterizado porque los datos biométricos se relacionan con una huella digital, las venas de la palma, el reconocimiento facial, el ADN, la impresión palmar, la geometría de la mano, el reconocimiento del iris, la retina, el olor, el andar o la voz.

31. (Nueva) Un método para proporcionar la verificación de la identidad personal multifactorial en base a la cadena de bloques, donde el método está implementado por medio de un sistema informático instalado en el servidor que comprende uno o más procesadores que ejecutan instrucciones de programas informáticos que, cuando se ejecutan, realizan el método, el método está caracterizado porque comprende:

- almacenar, mediante el sistema informático instalado en el servidor, una cadena de bloques en uno o más medios de almacenamiento legibles por computadora del sistema informático instalado en el servidor;

- asignar, mediante el sistema informático instalado en el servidor, una dirección de verificación asociada con la cadena de bloques a un individuo, donde el individuo tiene una identidad personal previamente verificada;

- almacenar, mediante el sistema informático instalado en el servidor, en uno o más medios de almacenamiento legibles por computadora, un identificador del individuo y el resumen biométrico del individuo en asociación con la dirección de verificación asociada con la cadena de bloques,

 - donde el resumen biométrico es un resumen de los datos biométricos del individuo, y donde cada uno del identificador, el resumen biométrico y la dirección de verificación son diferentes entre sí y son diferentes de las llaves privadas y públicas de las cuales derivó la dirección de verificación;

- obtener, mediante el sistema informático instalado en el servidor, de un dispositivo del cliente, el identificador y los datos biométricos en conexión con una solicitud para verificar la identidad del individuo, donde la solicitud indica la dirección de verificación asociada con la cadena de bloques;

- obtener, mediante el sistema informático instalado en el servidor, el identificador almacenado y el resumen biométrico almacenado con el uso de la dirección de verificación indicada en la solicitud; y

- asignar, mediante el sistema informático instalado en el servidor, la verificación de la identidad del individuo en respuesta a una determinación de que el identificador de la solicitud y los datos biométricos de la solicitud coinciden con el identificador almacenado y el resumen biométrico almacenado.

32. (Nueva) El método de acuerdo con la reivindicación 31, caracterizado porque comprende:

- firmar, mediante el sistema informático instalado en el servidor, con el uso de la llave privada de la cual derivó la dirección de verificación, la verificación de la identidad del individuo en respuesta a la determinación de que el identificador de la solicitud y los datos biométricos de la solicitud coinciden con el identificador almacenado y el resumen biométrico almacenado.

33. **(Nueva)** El método de acuerdo con la reivindicación 32, caracterizado porque comprende:
almacenar, mediante el sistema informático instalado en el servidor, en uno o más medios de almacenamiento legibles por computadora, la llave privada en asociación con la dirección de verificación asociada con la cadena de bloques,
obtener, mediante el sistema informático instalado en el servidor, del dispositivo del cliente, la llave privada en conexión con la solicitud para verificar la identidad del individuo;
obtener la llave privada almacenada con el uso de la dirección de verificación indicada en la solicitud; y
firmar, mediante el sistema informático instalado en el servidor, con el uso de la llave privada, la verificación de la identidad del individuo en respuesta a una determinación de que el identificador de la solicitud, los datos biométricos de la solicitud, y la llave privada de la solicitud coinciden con el identificador almacenado, el resumen biométrico almacenado y la llave privada almacenada.
34. **(Nueva)** El método de acuerdo con la reivindicación 31, caracterizado porque comprende:
asignar, mediante el sistema informático instalado en el servidor, otra dirección de verificación asociada con la cadena de bloques al individuo;
almacenar, mediante el sistema informático instalado en el servidor, en uno o más medios de almacenamiento legibles por computadora, otro resumen biométrico del individuo en asociación con la otra dirección de verificación asociada con la cadena de bloques, donde el otro resumen biométrico es un resumen de otros datos biométricos del individuo;
obtener, mediante el sistema informático instalado en el servidor, del dispositivo del cliente, los otros datos biométricos en conexión con la solicitud para verificar la identidad del individuo, donde la solicitud indica, además, la otra dirección de verificación asociada con la cadena de bloques;
obtener, mediante el sistema informático instalado en el servidor, el otro resumen biométrico almacenado con el uso de la otra dirección de verificación indicada en la solicitud; y
firmar, mediante el sistema informático instalado en el servidor, la verificación de la identidad del individuo en respuesta a una determinación de que el identificador de la solicitud, los datos biométricos de la solicitud, y los otros datos biométricos de la solicitud coinciden con el identificador almacenado, el resumen biométrico almacenado y el otro resumen biométrico almacenado.

35. (Nueva) El método de acuerdo con la reivindicación 34, caracterizado porque comprende:
obtener, mediante el sistema informático instalado en el servidor, a través de una interfaz de usuario, un comando iniciado por el usuario para agregar la otra dirección de verificación como dirección de la cadena de bloques para el individuo; y
asignar, mediante el sistema informático instalado en el servidor, la otra dirección de verificación asociada con la cadena de bloques al individuo en base al comando iniciado por el usuario.
36. (Nueva) El método de acuerdo con la reivindicación 34, caracterizado porque comprende:
obtener, mediante el sistema informático instalado en el servidor, a través de una interfaz de usuario, un comando iniciado por el usuario para quitar la otra dirección de verificación como dirección de la cadena de bloques para el individuo; y
desasociar, mediante el sistema informático instalado en el servidor, la otra dirección de verificación asociada con la cadena de bloques del individuo en base al comando iniciado por el usuario.
37. (Nueva) El método de acuerdo con la reivindicación 31, caracterizado porque comprende:
proporcionar, mediante el sistema informático instalado en el servidor, a un primer usuario, diferente del individuo, acceso a los datos almacenados en el uno o más medios de almacenamiento legibles por computadora en asociación con la dirección de verificación asociada con la cadena de bloques, donde al primer usuario se le brinda acceso a los datos almacenados en base a la verificación de que el primer usuario tiene una primera llave privada, donde la primera llave privada es diferente de la llave privada de la cual derivó la dirección de verificación; y
denegar, mediante el sistema informático instalado en el servidor, a un segundo usuario, distinto del individuo, acceso a los datos almacenados en base a la verificación de que el segundo usuario tiene una segunda llave privada.
38. (Nueva) El método de acuerdo con la reivindicación 31, caracterizado porque los datos biométricos comprenden una imagen, una grabación o un patrón.
39. (Nueva) El método de acuerdo con la reivindicación 31, caracterizado porque los datos biométricos se relacionan con una huella digital, las venas de la palma, el reconocimiento facial, el ADN, la impresión palmar, la geometría de la mano, el reconocimiento del iris, la retina, el olor, el andar o la voz.

40. (Nueva) Un sistema para proporcionar verificación de identidad personal multifactorial basada en cadena de bloques, caracterizado porque el sistema comprende:

uno o más medios de almacenamiento legibles por computadora para almacenar una cadena de bloques; un sistema informático instalado en un servidor que comprende uno o más procesadores programados para ejecutar instrucciones del programa informático que, cuando se ejecuta, hace que el sistema informático instalado en el servidor:

asignar múltiples direcciones de verificación de la cadena de bloques al individuo, donde el individuo tiene una identidad personal verificada previamente, donde 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;

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

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

donde cada uno del identificador, el primer resumen biométrico, el segundo resumen biométrico, la primera dirección de verificación y la segunda dirección de verificación son diferentes una de otra, diferentes de las primeras llaves privada y pública de las cuales derivó la primera dirección de verificación, y diferentes de las segundas llaves privada y pública de las cuales derivó la segunda dirección de verificación; obtener, de un dispositivo del cliente, el identificador, los primeros datos biométricos, y los segundos datos biométricos en conexión con una solicitud para verificar la identidad del individuo, donde la solicitud indica la primera dirección de verificación asociada con la cadena de bloques y la segunda dirección de verificación asociada con la cadena de bloques;

obtener (i) el identificador almacenado y el primer resumen biométrico almacenado, con el uso de la primera dirección de verificación indicada en la solicitud y (ii) el segundo resumen biométrico almacenado con el uso de la segunda dirección de verificación indicada en la solicitud; y

firmar, con el uso de la llave privada de la cual derivó la primera dirección de verificación,

la verificación de la identidad del individuo en respuesta a una determinación de que el identificador de la solicitud, los primeros datos biométricos de la solicitud, y los segundos datos biométricos de la solicitud coinciden con el identificador almacenado, el resumen biométrico almacenado y el segundo resumen biométrico almacenado;

proporcionar a un primer usuario, diferente del individuo, acceso a los datos almacenados en el uno o más medios de almacenamiento legibles por computadora en asociación con la primera dirección de verificación asociada con la cadena de bloques, donde al primer usuario se le brinda acceso a los datos almacenados en base a la verificación de que el primer usuario tiene una primera llave privada, donde la primera llave privada es diferente de la llave privada de la cual derivó la primera dirección de verificación y diferente de la llave privada de la cual derivó la segunda dirección de verificación; y

denegar a un segundo usuario, distinto del individuo, acceso a los datos almacenados en base a la verificación de que el segundo usuario tiene una segunda llave privada.

DIRECCIÓN DE NUEVAS CREACIONES
Procedimiento acelerado de exámenes de patente (PPH)

1	NÚMERO DE SOLICITUD ANTE LA SIC		
2	GLOBAL - PPH ☐ PAÍS	3	PCT – PPH ☐ PAÍS
4	PROSUR ☐ PAÍS	5	Alianza del Pacifico (AdP) ☐ PAÍS
6	OFICINA DE PRIMERA PRESENTACIÓN (OPP) ☒	7	OFICINA DE EXAMEN ANTERIOR (OEA) ☐
8	NÚMERO DE SOLICITUD O PUBLICACIÓN DE LA SOLICITUD (OPP) ☒ NÚMERO DE SOLICITUD EN OFICINA DE EXAMEN ANTERIOR (OEA): ☐ NÚMERO DE SOLICITUD PCT: ☐		1. US 15/083.241
9	☐ REPRESENTANTE LEGAL ☒ APODERADO		
APELLIDOS RAISBECK		NOMBRES J. IAN	IDENTIFICACIÓN C.C .79.376.996 de T.P .135.799 C.S.J Bogotá
DIRECCIÓN	Calle 90 No. 19-41 Oficina 404		No. TELÉFONO 7043275
CIUDAD	Bogotá		CORREO ELECTRÓNICO notificaciones.sic@roclaw.co
PAÍS	Colombia		No. RADICACIÓN O PROTOCOLO DE PODER GENERAL
10	CONDICIONES PARA ACCEDER A ESTE PROCESO:		
10.1. DATOS DE PRIORIDAD ☒ SI ☐ NO			
(33) PAÍS DE ORIGEN 1. ESTADOS UNIDOS DE AMERICA 2.		CÓDIGO PAÍS US	(31) NÚMERO 15/083.241 (32) FECHA (AAAA/MM/DD) 28 de marzo de 2016
10.2. DATOS SOLICITUD INTERNACIONAL PCT ☒ SI ☐ NO			
Solicitud Internacional No.		PCT/US2016/024776	Fecha 29 de marzo de 2016
Publicación Internacional No.		WO2017/171733	Fecha 5 de octubre de 2017
*El solicitante presenta una copia de la(s) reivindicación(es) patentable(s) u otorgable(s) de la solicitud de la Oficina de Primera Presentación que profirió el examen de patentabilidad, junto con una traducción al castellano. ☒ SI ☐ NO			
*El solicitante presenta los resultados de búsqueda de la Oficina de Examen Anterior, junto con una traducción al castellano ☒ SI ☐ NO			
REQUISITOS PARA EL RECONOCIMIENTO DE LOS RESULTADOS DE EXÁMENES DE PATENTABILIDAD EFECTUADOS A SOLICITUDES EXTRANJERAS			
Para que la Superintendencia de Industria y Comercio pueda reconocer los resultados de exámenes de patentabilidad producidos por otras Oficinas de Propiedad Industrial se debe cumplir con las siguientes condiciones:			
(a) Al momento de solicitar el examen de patentabilidad, si el solicitante pide que se reconozcan exámenes de patentabilidad de otras oficinas extranjeras, deberá aportar junto con el pago de la tasa correspondiente, los siguientes anexos:			
(i) Copia de las resoluciones, fallos o decisiones que han sido relevantes para la determinación de la patentabilidad de la(s) solicitud(es) en la Oficina que haya proferido el examen de patentabilidad que contienen reivindicaciones patentables u otorgables que son la base de la petición, y si es del caso, su traducción al castellano. ☒ SI ☐ NO			
(ii) Copia de todas las reivindicaciones determinadas como patentables u otorgables en la Oficina que profirió el examen de patentabilidad y, si es del caso, su traducción al castellano. ☒ SI ☐ NO			
(iii) Copia de los antecedentes, información o documentos citados por el examinador de la Oficina de Primera Presentación del examen de patentabilidad, en las resoluciones, fallos o decisiones correspondientes, incluyendo la literatura no patente. Los documentos de patente deberán presentarse siempre y cuando no estén disponibles para la Superintendencia de Industria y Comercio mediante el simple acceso a bases de datos gratuitas. ☐ SI ☒ NO			
(iv) Una tabla de correspondencias de las reivindicaciones que han sido determinadas como patentables u otorgables en la solicitud de la Oficina que haya proferido el examen de patentabilidad. ☒ SI ☐ NO			
11	FIRMA DEL SOLICITANTE, DEL APODERADO O DEL REPRESENTANTE LEGAL Junto a cada firma, indicar el nombre del firmante y su calidad (si tal calidad no es obvia al leer el petitorio)		

Sam Kimbark

6	TABLA DE CORRESPONDENCIA DE REIVINDICACIONES		
Reivindicaciones en la solicitud en Colombia		Reivindicaciones otorgables en la solicitud internacional	Explicación sobre la suficiente correspondencia ó Comentarios que explican la correspondencia
<i>Reivindicaciones 1 a 20 tal y como se modificaron el 29 de octubre de 2018.</i>		<i>Reivindicaciones 1 a 20 correspondientes a la patente US 9,985,964.</i>	<i>Las Reivindicaciones 1 a 20 modificadas el 29 de octubre de 2018 corresponden en su totalidad a las Reivindicaciones 1 a 20 otorgadas dentro de la patente Estadounidense US 9,985,964, para la solicitud No. 15/083241, sobre la que se reivindica prioridad en la presente solicitud de patente.</i>



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/083,241	05/29/2018	9985964	17-10153	5060

36212 7590 05/09/2018
HOFFMAN PATENT GROUP
28494 WESTINGHOUSE PLACE
SUITE 204
VALENCIA, CA 91355

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b) (application filed on or after May 29, 2000)

The Patent Term Adjustment is 143 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (<http://pair.uspto.gov>).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site <http://pair.uspto.gov> for additional applicants):

Marcus Andrade, Fernley, NV;
BLACK GOLD COIN, INC., Las Vegas, NV;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

909 7590 04/18/2018
Pillsbury Winthrop Shaw Pittman, LLP
PO Box 10500
McLean, VIRGINIA 22102
UNITED STATES OF AMERICA

EXAMINER

GOODCHILD, WILLIAM J

ART UNIT

PAPER NUMBER

2433

DATE MAILED: 04/18/2018

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/083,241	03/28/2016	Marcus Andrade	038918-0444639	5060

TITLE OF INVENTION: SYSTEMS AND METHODS FOR PROVIDING BLOCK CHAIN-BASED MULTIFACTOR PERSONAL IDENTITY VERIFICATION

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	\$500	\$0.00	\$0.00	\$500	07/18/2018

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: **Mail** **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

909 7590 04/18/2018
Pillsbury Winthrop Shaw Pittman, LLP
PO Box 10500
McLean, VIRGINIA 22102
UNITED STATES OF AMERICA

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/083,241	03/28/2016	Marcus Andrade	038918-0444639	5060

TITLE OF INVENTION: SYSTEMS AND METHODS FOR PROVIDING BLOCK CHAIN-BASED MULTIFACTOR PERSONAL IDENTITY VERIFICATION

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	\$500	\$0.00	\$0.00	\$500	07/18/2018

EXAMINER	ART UNIT	CLASS-SUBCLASS
GOODCHILD, WILLIAM J	2433	726-006000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____

2 _____

3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☐ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:

4b. Payment of Fee(s): (**Please first reapply any previously paid issue fee shown above**)

☐ Issue Fee

☐ A check is enclosed.

☐ Publication Fee (No small entity discount permitted)

☐ Payment by credit card. Form PTO-2038 is attached.

☐ Advance Order - # of Copies _____

☐ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

☐ Applicant certifying micro entity status. See 37 CFR 1.29

☐ Applicant asserting small entity status. See 37 CFR 1.27

☐ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____

Date _____

Typed or printed name _____

Registration No. _____



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/083,241	03/28/2016	Marcus Andrade	038918-0444639	5060
909	7590	04/18/2018	EXAMINER	
Pillsbury Winthrop Shaw Pittman, LLP			GOODCHILD, WILLIAM J	
PO Box 10500			ART UNIT	
McLean, VIRGINIA 22102			PAPER NUMBER	
UNITED STATES OF AMERICA			2433	

DATE MAILED: 04/18/2018

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b) (Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

<i>Notice Requiring Inventor's Oath or Declaration</i>	Application No. 15/083,241	Applicant(s) Marcus Andrade	
	Examiner GOODCHILD, WILLIAM J	Art Unit 2433	

This notice is an attachment to the Notice of Allowability (PTOL-37), or the Notice of Allowability For A Design Application (PTOL-37D).

An inventor's oath or declaration in compliance with 37 CFR 1.63 or 1.64 executed by or with respect to each inventor has not yet been submitted.

An oath or declaration in compliance with 37 CFR 1.63, or a substitute statement in compliance with 37 CFR 1.64, executed by or with respect to each inventor (for any inventor for which a compliant oath, declaration, or substitute statement has not yet been submitted) **MUST** be filed no later than the date on which the issue fee is paid. See 35 U.S.C. 115(f). Failure to timely comply will result in ABANDONMENT of this application.

A properly executed inventor's oath to declaration has not been received for the following inventor(s):

If applicant previously filed one or more oaths, declarations, or substitute statements, applicant may have received an informational notice regarding deficiencies therein.

The following deficiencies are noted:

INFORMAL ACTION PROBLEMS

- A properly executed inventor's oath or declaration has not been received for the following inventor(s): **Marcus Andrade**.

Applicant may submit the inventor's oath or declaration at any time before the Notice of Allowance and Fee(s) Due, PTOL-85, is mailed.

Questions relating to this Notice should be directed to the Application Assistance Unit at 571-272-4200.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 15/083,241	Applicant(s) Andrade, Marcus	
	Examiner WILLIAM J GOODCHILD	Art Unit 2433	AIA Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 12/19/2017.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on ____.

2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on ____; the restriction requirement and election have been incorporated into this action.

3. ☒ The allowed claim(s) is/are 21-40. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a) ☐ All b) ☐ Some *c) ☐ None of the:

1. ☐ Certified copies of the priority documents have been received.

2. ☐ Certified copies of the priority documents have been received in Application No. ____.

3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: ____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date ____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892) 2. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date ____. 3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material ____. 4. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____.	5. ☐ Examiner's Amendment/Comment 6. ☒ Examiner's Statement of Reasons for Allowance 7. ☐ Other _____.
---	--

/William J. Goodchild/
Primary Examiner, Art Unit 2433

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

Response to Arguments

2. Applicant's arguments, see Remarks, filed 12/19/2017, with respect to claims 21-40 have been fully considered and are persuasive. The 102/103 rejections have been withdrawn.

Allowable Subject Matter

3. Claims 21-40 are allowed.

4. The following is an examiner's statement of reasons for allowance: amended independent claims relating to "wherein each of the identifier, the biometric hash, and the verification address are different from one another and different from private and public keys from which the verification address was derived;" and "obtain, from a client-side device, the identifier and the biometric data in connection with a request to verify the individual's identity, the request indicating the verification address of the blockchain" are not found within the art of record.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably

accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to WILLIAM J GOODCHILD whose telephone number is (571)270-1589. The examiner can normally be reached on M-F 8am-4:30pm.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at <http://www.uspto.gov/interviewpractice>.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jeff Pwu can be reached on 571-272-6798. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

Application/Control Number: 15/083,241
Art Unit: 2433

Page 4

USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/William J. Goodchild/
Primary Examiner, Art Unit 2433

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

In Re Patent Application Of:	Marcus ANDRADE	)	Attorney Docket No.:	038918-0444639
Serial No.:	15/083,241	)	Confirmation No.:	5060
Filing Date:	March 28, 2016	)	Examiner:	William J. Goodchild
		)	Art Unit:	2433

For: SYSTEM AND METHOD FOR PROVIDING BLOCKCHAIN-BASED
MULTIFACTOR PERSONAL IDENTITY VERIFICATION

**RESPONSE TO NON-FINAL OFFICE ACTION
MAILED 18 OCTOBER 2017****MAIL STOP AMENDMENT**

Commissioner for Patents
P.O. Box 1450
Alexandria, VA. 22313-1450

Dear Sir:

In response to the Non-Final Office Action mailed **October 18, 2017** (hereinafter "Office Action"), please amend the above- identified application as follows:

Amendments to the Claims begin on page 2 of this paper.

Remarks begin on page 10 of this paper.

It is not believed that extensions of time or fees for net addition of claims are required beyond those that may otherwise be provided for in documents accompanying this paper. However, if additional extensions of time are necessary to prevent abandonment of this application, then such extensions of time are hereby petitioned for under 37 C.F.R. § 1.136(a), and any fees required therefore (including fees for net addition of claims) are hereby authorized to be charged to Deposit Account No. 033975 (**Ref. No. 038918-0444639**).

This listing of claims will replace all prior versions and listings of claims in the Application.

LISTING OF CLAIMS:

1-20. (Cancelled)

21. (New) A system for providing blockchain-based multifactor personal identity verification, the system comprising:

one or more computer-readable storage media configured to store a blockchain;

a server-side computer system comprising one or more processors programmed to execute computer program instructions that, when executed, cause the server-side computer system to:

assign a verification address associated with the blockchain to an individual, the individual having a previously verified personal identity;

store, at the one or more computer-readable storage media, an identifier of the individual and a biometric hash of the individual in association with the verification address associated with the blockchain,

wherein the biometric hash is a hash of biometric data of the individual,
and

wherein each of the identifier, the biometric hash, and the verification address are different from one another and different from private and public keys from which the verification address was derived;

obtain, from a client-side device, the identifier and the biometric data in connection with a request to verify the individual's identity, the request indicating the verification address associated with the blockchain;

obtain the stored identifier and the stored biometric hash using the verification address indicated in the request; and

sign verification of the individual's identity responsive to a determination that the identifier of the request and the biometric data of the request match the stored identifier and the stored biometric hash.

22. (New) The system of claim 21, wherein the server-side computer system is caused to:
sign, using the private key from which the verification address was derived, the verification of the individual's identity responsive to the determination that the identifier of the request and the biometric data of the request match the stored identifier and the stored biometric hash.
23. (New) The system of claim 22, wherein the server -side computer system is caused to:
store, at the one or more computer-readable storage media, the private key in association with the verification address associated with the blockchain;
obtain, from the client-side device, the private key in connection with the request to verify the individual's identity;
obtain the stored private key using the verification address indicated in the request; and
sign, using the private key, the verification of the individual's identity responsive to a determination that the identifier of the request, the biometric data of the request, and the private key of the request match the stored identifier, the stored biometric hash, and the stored private key.
24. (New) The system of claim 23, wherein the private key is also stored on the client-side device, and wherein the client-side device is a user device of the individual.
25. (New) The system of claim 21, wherein the server-side computer system is caused to:
assign another verification address associated with the blockchain to the individual;
store, at the one or more computer-readable storage media, another biometric hash of the individual in association with the other verification address associated with the blockchain, the other biometric hash being a hash of other biometric data of the individual;
obtain, from the client-side device, the other biometric data in connection with the request to verify the individual's identity, the request further indicating the other verification address associated with the blockchain;
obtain the stored other biometric hash using the other verification address indicated in the request; and

sign the verification of the individual's identity responsive to a determination that the identifier of the request, the biometric data of the request, the other biometric data of the request match the stored identifier, the stored biometric hash, and the stored other biometric hash.

26. (New) The system of claim 25, wherein the server-side computer system is caused to:
obtain, via a user interface, a user-initiated command to add the other verification address as an address of the blockchain for the individual; and
assign the other verification address associated with the blockchain to the individual based on the user-initiated command.

27. (New) The system of claim 25, wherein the server-side computer system is caused to:
obtain, via a user interface, a user-initiated command to remove the other verification address as an address of the blockchain for the individual; and
de-associate the other verification address associated with the blockchain from the individual based on the user-initiated command.

28. (New) The system of claim 21, wherein the server-side computer system is caused to:
provide a first user, different than the individual, access to data stored at the one or more computer-readable storage media in association with the verification address associated with the blockchain, the first user being provided access to the stored data based on verification that the first user has a first private key, the first private key being different the private key from which the verification address was derived; and
denying a second user, different than the individual, access to the stored data based on verification that the second user has a second private key.

29. (New) The system of claim 21, wherein the biometric data comprises an image, a recording, or a template.

30. (New) The system of claim 21, wherein the biometric data is related to a fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina, odor, gait, or voice.

31. (New) A method of providing blockchain-based multifactor personal identity verification, the method being implemented by a server-side computer system comprising one or more processors executing computer program instructions that, when executed, perform the method, the method comprising:

storing, by the server-side computer system, a blockchain at one or more computer-readable storage media of the server-side computer system;

assigning, by the server-side computer system, a verification address associated with the blockchain to an individual, the individual having a previously verified personal identity;

storing, by the server-side computer system, at the one or more computer-readable storage media, an identifier of the individual and a biometric hash of the individual in association with the verification address associated with the blockchain,

wherein the biometric hash is a hash of biometric data of the individual, and

wherein each of the identifier, the biometric hash, and the verification address are different from one another and different from private and public keys from which the verification address was derived;

obtaining, by the server-side computer system, from a client-side device, the identifier and the biometric data in connection with a request to verify the individual's identity, the request indicating the verification address associated with the blockchain;

obtaining, by the server-side computer system, the stored identifier and the stored biometric hash using the verification address indicated in the request; and

assigning, by the server-side computer system, verification of the individual's identity responsive to a determination that the identifier of the request and the biometric data of the request match the stored identifier and the stored biometric hash.

32. (New) The method of claim 31, comprising:

signing, by the server-side computer system, using the private key from which the verification address was derived, the verification of the individual's identity responsive to the

determination that the identifier of the request and the biometric data of the request match the stored identifier and the stored biometric hash.

33. (New) The method of claim 32, comprising:

storing, by the server-side computer system, at the one or more computer-readable storage media, the private key in association with the verification address associated with the blockchain;

obtaining, by the server-side computer system, from the client-side device, the private key in connection with the request to verify the individual's identity;

obtaining the stored private key using the verification address indicated in the request; and

signing, by the server-side computer system, using the private key, the verification of the individual's identity responsive to a determination that the identifier of the request, the biometric data of the request, and the private key of the request match the stored identifier, the stored biometric hash, and the stored private key.

34. (New) The method of claim 31, comprising:

assigning, by the server-side computer system, another verification address associated with the blockchain to the individual;

storing, by the server-side computer system, at the one or more computer-readable storage media, another biometric hash of the individual in association with the other verification address associated with the blockchain, the other biometric hash being a hash of other biometric data of the individual;

obtaining, by the server-side computer system, from the client-side device, the other biometric data in connection with the request to verify the individual's identity, the request further indicating the other verification address associated with the blockchain;

obtaining, by the server-side computer system, the stored other biometric hash using the other verification address indicated in the request; and

signing, by the server-side computer system, the verification of the individual's identity responsive to a determination that the identifier of the request, the biometric data of the request, the other biometric data of the request match the stored identifier, the stored biometric hash, and the stored other biometric hash.

35. (New) The method of claim 34, comprising:

obtaining, by the server-side computer system, via a user interface, a user-initiated command to add the other verification address as an address of the blockchain for the individual; and

assigning, by the server-side computer system, the other verification address associated with the blockchain to the individual based on the user-initiated command.

36. (New) The method of claim 34, comprising:

obtaining, by the server-side computer system, via a user interface, a user-initiated command to remove the other verification address as an address of the blockchain for the individual; and

de-associating, by the server-side computer system, the other verification address associated with the blockchain from the individual based on the user-initiated command.

37. (New) The method of claim 31, comprising:

providing, by the server-side computer system, a first user, different than the individual, access to data stored at the one or more computer-readable storage media in association with the verification address associated with the blockchain, the first user being provided access to the stored data based on verification that the first user has a first private key, the first private key being different the private key from which the verification address was derived; and

denying, by the server-side computer system, a second user, different than the individual, access to the stored data based on verification that the second user has a second private key.

38. (New) The method of claim 31, wherein the biometric data comprises an image, a recording, or a template.

39. (New) The method of claim 31, wherein the biometric data is related to a fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina, odor, gait, or voice.

40. (New) A system for providing blockchain-based multifactor personal identity verification, the system comprising:

one or more computer-readable storage media configured to store a blockchain;

a server-side computer system comprising one or more processors programmed to execute computer program instructions that, when executed, cause the server-side computer system to:

assign multiple verification addresses of the blockchain to the individual, the individual having a previously verified personal identity, the multiple verification addresses include a first verification address associated with the blockchain and a second verification address associated with the blockchain;

store, at the one or more computer-readable storage media, (i) an identifier of the individual and a first biometric hash of the individual in association with the first verification address associated with the blockchain and (ii) a second biometric hash of the individual in association with the second verification address associated with the blockchain,

wherein the first biometric hash is a hash of first biometric data of the individual, and the second biometric hash is a hash of second biometric data of the individual, and

wherein each of the identifier, the first biometric hash, the second biometric hash, the first verification address, and the second verification address are different from one another, different from first private and public keys from which the first verification address was derived, and different from second private and public keys from which the second verification address was derived;

obtain, from a client-side device, the identifier, the first biometric data, and the second biometric data in connection with a request to verify the individual's identity, the request indicating the first verification address associated with the blockchain and the second verification address associated with the blockchain;

obtain (i) the stored identifier and the stored first biometric hash using the first verification address indicated in the request and (ii) the stored second biometric hash using the second verification address indicated in the request; and

sign, using the private key from which the first verification address was derived,

verification of the individual's identity responsive to a determination that the identifier of the request, the first biometric data of the request, and the second biometric data of the request match the stored identifier, the stored first biometric hash, and the stored second biometric hash;

provide a first user, different than the individual, access to data stored at the one or more computer-readable storage media in association with the first verification address associated with the blockchain, the first user being provided access to the stored data based on verification that the first user has a first private key, the first private key being different the private key from which the first verification address was derived and different from the private key from which the second verification address was derived; and

deny a second user, different than the individual, access to the stored data based on verification that the second user has a second private key.

REMARKS

By this response, claims 1-20 have been cancelled without prejudice or disclaimer, and claims 21-40 have been newly added. Therefore, claims 21-40 are now pending. Support for the instant amendments is provided throughout the as-filed Specification. Thus, no new matter has been added. In view of the foregoing amendments and following comments, allowance of all the claims pending in the application is respectfully requested.

35 U.S.C. §§ 102/103 REJECTIONS

Applicant disagrees with the propriety of the prior art rejection. Nevertheless, solely to expedite prosecution of this case, Applicant has amended the set of pending claims. The references relied-upon in the Office Action fail to teach or suggest the set of pending claims (as at least currently amended). As an example, U.S. Patent Application Publication No. 2015/0324789 to Dvorak *et al.* (“Dvorak”) fails to teach the following features of claim 1:

a server-side computer system [caused to]:

assign a verification address associated with the blockchain to an individual...;

store, at the ... computer-readable storage media [of the server-side computer system], an identifier of the individual and a biometric hash of the individual in association with the verification address associated with the blockchain,

wherein the biometric hash is a hash of biometric data of the individual, and

wherein each of the identifier, the biometric hash, and the verification address are different from one another and different from private and public keys from which the verification address was derived;

obtain, from a client-side device, the identifier and the biometric data in connection with a request to verify the individual's identity, the request indicating the verification address associated with the blockchain; ... and

sign verification of the individual's identity responsive to a determination that the identifier of the request and the biometric data of the request match the stored identifier and the stored biometric hash.

Independent claims 31 and 40 include similar recitations.

No other relied-upon reference overcomes the foregoing deficiencies of Dvorak. The Office Action does not allege otherwise.

For at least the foregoing reasons, Applicant respectfully request withdrawal of the prior art rejections. The dependent claims are also allowable because they each ultimately depend from an allowable independent claim, as well as for the further features they recite.

CONCLUSION

Having addressed each of the foregoing rejections, it is respectfully submitted that a full and complete response has been made to the outstanding Office Action and, as such, the application is in condition for allowance. Notice to that effect is respectfully requested.

If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at the number provided.

Respectfully submitted,

Date: **December 19, 2017**

PILLSBURY WINTHROP SHAW PITTMAN LLP

By: /Ngai B. Zhang/
Ngai B. Zhang
Registration No. 65,473

Customer No. 00909

P.O.Box 10500
McLean, Virginia 22102
Direct Dial: 703.770.7532
Main: 703.770.7900
Fax: 703.770.7901



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/083,241	03/28/2016	Marcus Andrade	038918-0444639	5060

909 7590 10/18/2017
Pillsbury Winthrop Shaw Pittman, LLP
PO Box 10500
McLean, VA 22102

EXAMINER

GOODCHILD, WILLIAM J

ART UNIT	PAPER NUMBER
----------	--------------

2433

NOTIFICATION DATE	DELIVERY MODE
-------------------	---------------

10/18/2017

ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docket_ip@pillsburylaw.com

Office Action Summary	Application No. 15/083,241	Applicant(s) ANDRADE, MARCUS	
	Examiner WILLIAM GOODCHILD	Art Unit 2433	AIA (First Inventor to File) Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 03/28/2016.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on ____.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on ____; the restriction requirement and election have been incorporated into this action.
- 4) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

- 5) ☒ Claim(s) 1-20 is/are pending in the application.
5a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 6) ☐ Claim(s) ____ is/are allowed.
- 7) ☒ Claim(s) 1-20 is/are rejected.
- 8) ☐ Claim(s) ____ is/are objected to.
- 9) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

- 10) ☐ The specification is objected to by the Examiner.
- 11) ☐ The drawing(s) filed on ____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

- a) ☐ All b) ☐ Some** c) ☐ None of the:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. ____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☒ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b)
Paper No(s)/Mail Date 09/19/2016
- 3) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____.
- 4) ☐ Other: ____.

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(a)(1) the claimed invention was patented, described in a printed publication, or in public use, on sale or otherwise available to the public before the effective filing date of the claimed invention.

(a)(2) the claimed invention was described in a patent issued under section 151, or in an application for patent published or deemed published under section 122(b), in which the patent or application, as the case may be, names another inventor and was effectively filed before the effective filing date of the claimed invention.

2. Claim(s) 1-3, 5-15 and 17-20 are rejected under 35 U.S.C. 102(a)(1) and (a)(2) as being anticipated by Dvorak et al., (US Publication No. 2015/0324789), hereinafter “Dvorak”.

Regarding claims 1, 14 and 18, Dvorak discloses

providing block chain-based multifactor personal identity verification [Dvorak, Abstract and paragraph 60]:

one or more hardware processors configured by machine-readable instructions [Dvorak, paragraphs 58 and 59] to:

Art Unit: 2433

establish verification addresses on a block chain by: associating identifiers with individuals having previously verified personal identities, a first identifier being associated a first individual, the first individual having a previously verified personal identity [Dvorak, paragraphs 60, 62-64, 111 and 112];

assigning verification addresses on a block chain to the individuals, a given verification address including a public key and a private key, a first verification address being assigned to the first individual, the first verification address including a first public key and a first private key [Dvorak, paragraphs 59, 112 and 113]; and

recording identifiers and biometric data associated with the individuals at corresponding verification addresses, the first identifier and first biometric data associated with the first individual being recorded at the first verification address [Dvorak, paragraphs 94 and 98]; and

perform block chain-based multifactor personal identity verification using the verification addresses [Dvorak, paragraph 59] by: receiving one or more identifiers in connection with one or more requests to verify an identity of one or more individuals, the first identifier being received in connection with a request to verify an identity of the first individual [Dvorak, paragraphs 58, 62-65, 72 and 94];

extracting the biometric data associated with the one or more individuals from the corresponding verification addresses, the first biometric data associated with the first individual being extracted from the first verification address [Dvorak, paragraphs 58 and 67]; and

Art Unit: 2433

verifying the identity of the one or more individuals upon receiving matching biometric data and private keys, the personal identity of the first individual being verified upon receipt of (1) biometric data matching the first biometric data and (2) a private key matching the first private key [Dvorak, paragraphs 57, 67 and 94].

Regarding claim 2, Dvorak further discloses wherein the first private key is stored within a computing platform associated with the first individual [Dvorak, paragraph 67].

Regarding claims 3 and 15, Dvorak further discloses wherein multiple verification addresses are assigned to separate individuals such that, in addition to the first verification address, a second verification address is assigned to the first individual [Dvorak, paragraph 59].

Regarding claims 5 and 17, Dvorak further discloses wherein different biometric data is recorded at multiple verification addresses assigned to a given individual such that, in addition to the first identifier and the first biometric data associated with the first individual being recorded at the first verification address, the first identifier and second biometric data associated with the first individual is recorded at the second verification address [Dvorak, paragraphs 59, 84 and 98].

Art Unit: 2433

Regarding claim 6, Dvorak further discloses

wherein the personal identity of the first individual being verified upon receipt of (1) biometric data matching the first biometric data or the second biometric data and (2) a private key matching the first private key [Dvorak, paragraphs 90, 51, 94 and 59].

Regarding claim 7, Dvorak further discloses

wherein the biometric data includes one or more of an image, a recording, or a template [Dvorak, paragraph 59].

Regarding claim 8, Dvorak further discloses

wherein the biometric data is related to one or more of a fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina, odor or scent, typing rhythm, gait, or voice [Dvorak, paragraphs 90 and 51].

Regarding claim 9, Dvorak further discloses

wherein the first biometric data is received via a computing platform associated with the first individual [Dvorak, paragraph 67].

Regarding claim 10, Dvorak further discloses

wherein the one or more hardware processors are further configured by machine-readable instructions to, responsive to receiving the request to verify the identity of the first individual, prompt the first individual for biometric data matching the first biometric

Art Unit: 2433

data and a private key matching the first private key, the prompt being conveyed via a computing platform associated with the first individual [Dvorak, paragraphs 90, 51 and 67].

Regarding claim 11, Dvorak further discloses

wherein the one or more hardware processors are further configured by machine-readable instructions to, responsive to receiving the request to verify the identity of the first individual, prompt a computing platform associated with the first individual to automatically provide biometric data matching the first biometric data and a private key matching the first private key [Dvorak, paragraphs 90, 51, 94 and 67].

Regarding claims 12 and 20, Dvorak further discloses

wherein the biometric data matching the first biometric data and the private key matching the first private key are used to sign the verification of the personal identity of the first individual [Dvorak, paragraph 51].

Regarding claim 13, Dvorak further discloses

wherein at least one dedicated node performs the signing of the verification of the personal identity of the first individual [Dvorak, paragraph 52].

Regarding claim 19, Dvorak further discloses

responsive to receiving the request to verify the identity of the first individual: prompting the first individual for biometric data matching the first biometric data and a private key matching the first private key, the prompt being conveyed via a computing platform associated with the first individual [Dvorak, paragraphs 90, 51 and 67]; or prompting a computing platform associated with the first individual to automatically provide biometric data matching the first biometric data and a private key matching the first private key [Dvorak, paragraphs 90, 51, 94 and 67].

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103 which forms the basis for all obviousness rejections set forth in this Office action:

A patent for a claimed invention may not be obtained, notwithstanding that the claimed invention is not identically disclosed as set forth in section 102, if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 4 and 16 are rejected under 35 U.S.C. 103 as being unpatentable over Dvorak as applied to claims 1 and 14 above, and further in view of Pennanen, (US Publication No. 2015/0356555).

Regarding claims 4 and 16, Dvorak further discloses wherein the one or more hardware processors are further configured by machine-readable instructions to provide an interface for presentation to individuals via associated computing platforms [Dvorak, paragraph 58].

Dvorak does not specifically disclose the interface being configured to allow a given individual to add or delete verification addresses assigned to the given individual so long as at least one verification address is assigned to the given individual.

However, Pennanen teaches a system implementing at least one cryptocurrency transaction at a point-of-sale by using a mobile terminal [Pennanen, Abstract] and discloses to add or delete verification addresses assigned to the given individual so long as at least one verification address is given [Pennanen, paragraph 68 and figure 2].

It would have been obvious to one having ordinary skill in the art before the effective filing date of the claimed invention to use the keys of Pennanen to add and delete addresses of an individual in the bitcoin system of Case in order to authenticate the cryptocurrency.

Conclusion

Examiner's Note: Examiner has cited particular paragraphs / columns and line numbers in the reference(s) applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings of the art and are applied to specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant in preparing

Art Unit: 2433

responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the cited passages as taught by the prior art or relied upon by the examiner.

Should applicant amend the claims of the claimed invention, it is respectfully requested that applicant clearly indicate the portion(s) of applicant's specification that support the amended claim language for ascertaining the metes and bounds of applicant's claimed invention.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to WILLIAM GOODCHILD whose telephone number is (571)270-1589. The examiner can normally be reached on Monday - Friday / 8:00 AM - 4:00 PM EST.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at <http://www.uspto.gov/interviewpractice>.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jeffrey Pwu can be reached on (571) 272-6798. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2433

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/WILLIAM GOODCHILD/
Primary Examiner, Art Unit 2433



US009985964B2

(12) **United States Patent**
Andrade

(10) **Patent No.:** **US 9,985,964 B2**
(45) **Date of Patent:** **May 29, 2018**

(54) **SYSTEMS AND METHODS FOR PROVIDING
BLOCK CHAIN-BASED MULTIFACTOR
PERSONAL IDENTITY VERIFICATION**

(71) Applicant: **BLACK GOLD COIN, INC.**, Las
Vegas, NV (US)

(72) Inventor: **Marcus Andrade**, Fernley, NV (US)

(73) Assignee: **Black Gold Coin, Inc.**, Las Vegas, NV
(US)

(*) Notice: Subject to any disclaimer, the term of this
patent is extended or adjusted under 35
U.S.C. 154(b) by 143 days.

(21) Appl. No.: **15/083,241**

(22) Filed: **Mar. 28, 2016**

(65) **Prior Publication Data**

US 2017/0279801 A1 Sep. 28, 2017

(51) **Int. Cl.**
H04L 29/06 (2006.01)

(52) **U.S. Cl.**
CPC **H04L 63/0861** (2013.01)

(58) **Field of Classification Search**
None
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2012/0084563 A1* 4/2012 Singhal G06F 21/32
713/168

2015/0178693 A1 6/2015 Solis

2015/0324789 A1* 11/2015 Dvorak G06Q 20/3823
705/67

2015/0356555 A1* 12/2015 Pennanen G06Q 20/06
705/71

2017/0317997 A1* 11/2017 Smith H04L 63/061

OTHER PUBLICATIONS

PCT International Application No. PCT/US2016/024776; International Search Report and Written Opinion, dated Jun. 16, 2016. (13 pages).

* cited by examiner

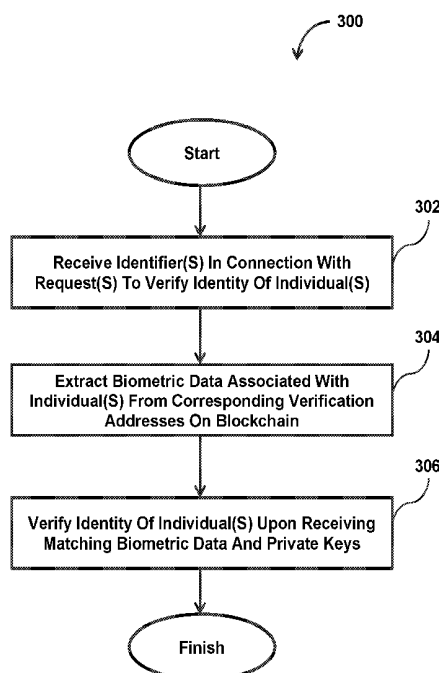
Primary Examiner — William J. Goodchild

(74) *Attorney, Agent, or Firm* — David L. Hoffman;
Hoffman Patent Group

(57) **ABSTRACT**

Block chain-based multifactor personal identity verification may be provided. Verification addresses may be established on a block chain by: associating identifiers with individuals having previously verified personal identities, assigning verification addresses on a block chain to the individuals, and recording identifiers and biometric data associated with the individuals at corresponding verification addresses. Block chain-based multifactor personal identity verification using the verification addresses may be performed by: receiving one or more identifiers in connection with one or more requests to verify an identity of one or more individuals, extracting the biometric data associated with the one or more individuals from the corresponding verification addresses, and verifying the identity of the one or more individuals upon receiving matching biometric data and private keys.

20 Claims, 3 Drawing Sheets



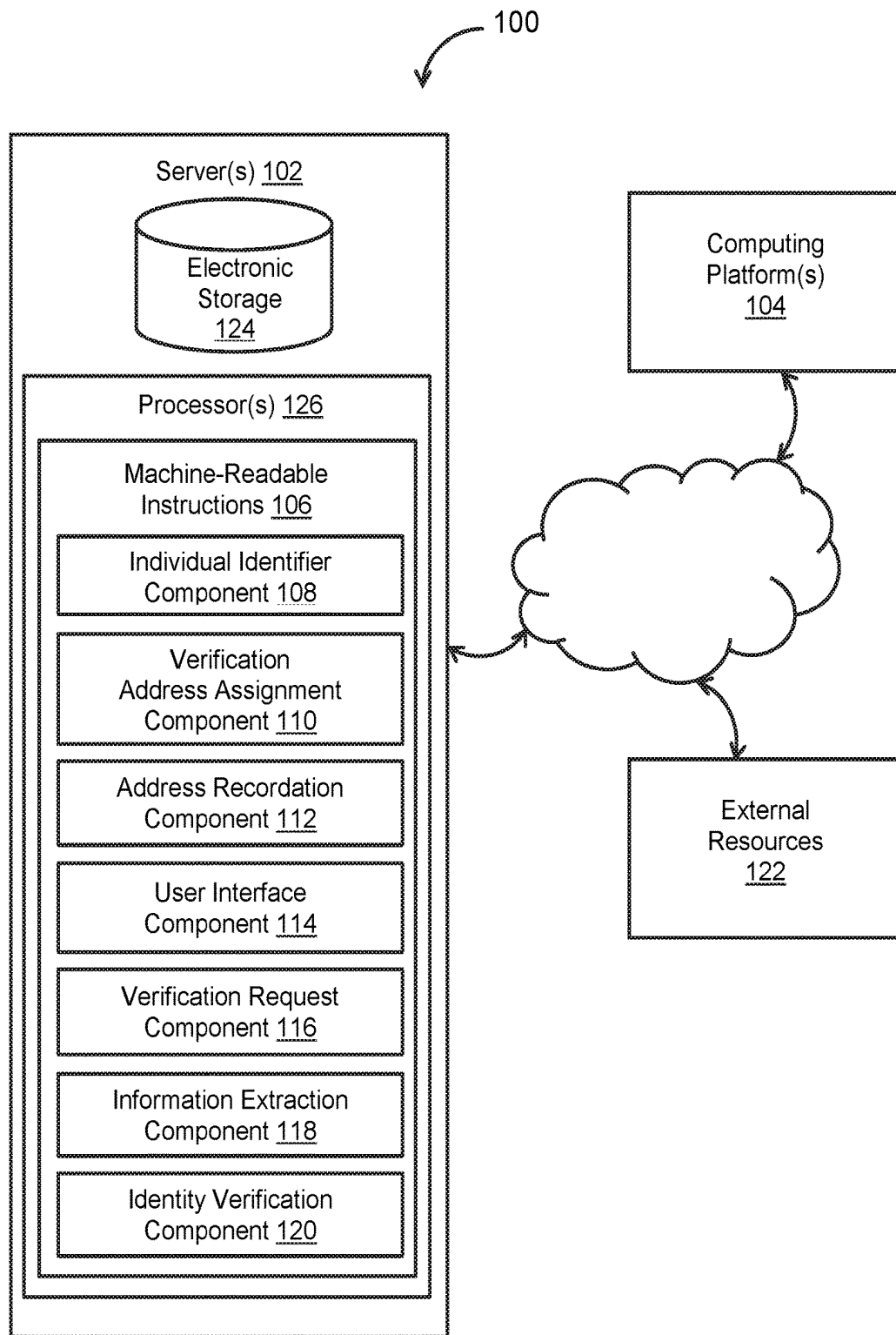
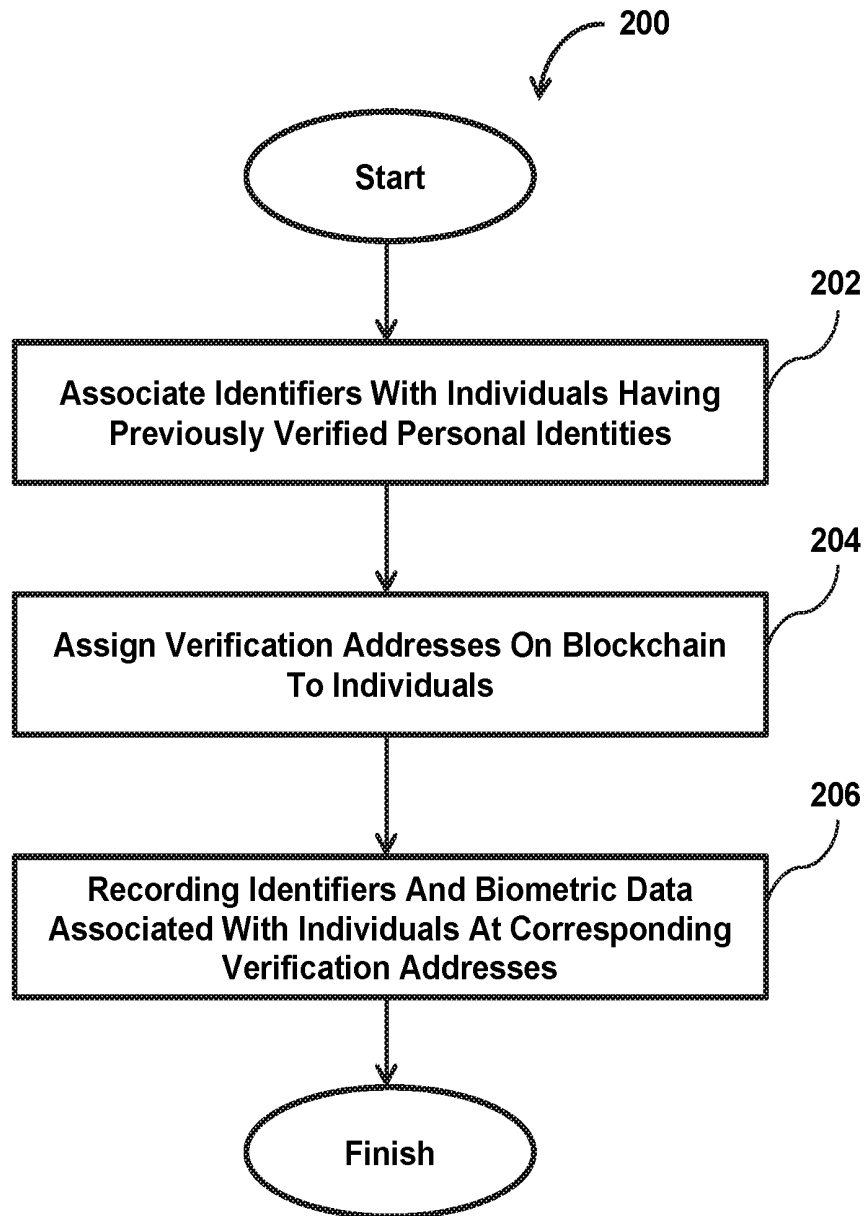
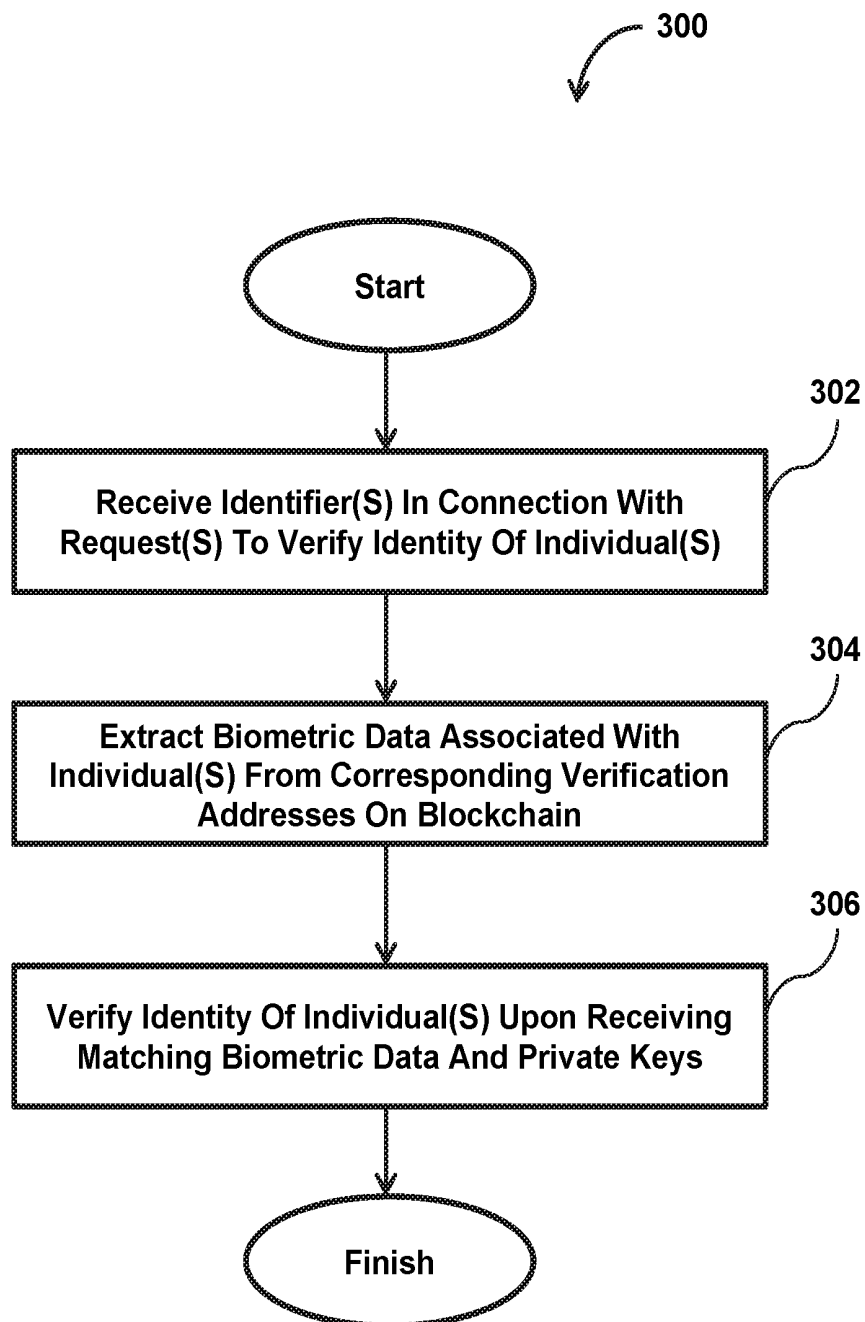


FIG. 1

**FIG. 2**

**FIG. 3**

SYSTEMS AND METHODS FOR PROVIDING BLOCK CHAIN-BASED MULTIFACTOR PERSONAL IDENTITY VERIFICATION

FIELD OF THE DISCLOSURE

This disclosure relates to systems and methods for providing block chain-based multifactor personal identity verification.

SUMMARY

One aspect of the disclosure relates to a system for providing block chain-based multifactor personal identity verification. The system may include one or more hardware processors configured by machine-readable instructions to establish verification addresses on a block chain and/or perform block chain-based multifactor personal identity verification using the verification addresses. Establishing verification addresses on the block chain may include associating identifiers with individuals having previously verified personal identities, a first identifier being associated a first individual, the first individual having a previously verified personal identity; assigning verification addresses on a block chain to the individuals, a given verification address including a public key and a private key, a first verification address being assigned to the first individual, the first verification address including a first public key and a first private key; and recording identifiers and biometric data associated with the individuals at corresponding verification addresses, the first identifier and first biometric data associated with the first individual being recorded at the first verification address. Performing block chain-based multifactor personal identity verification using the verification addresses may include receiving one or more identifiers in connection with one or more requests to verify an identity of one or more individuals, the first identifier being received in connection with a request to verify an identity of the first individual; extracting the biometric data associated with the one or more individuals from the corresponding verification addresses, the first biometric data associated with the first individual being extracted from the first verification address; and verifying the identity of the one or more individuals upon receiving matching biometric data and private keys, the personal identity of the first individual being verified upon receipt of (1) biometric data matching the first biometric data and (2) a private key matching the first private key.

Another aspect of the disclosure relates to a method for establishing verification addresses on a block chain in order to provide block chain-based multifactor personal identity verification. The method may be performed by one or more hardware processors configured by machine-readable instructions. The method may include associating identifiers with individuals having previously verified personal identities, a first identifier being associated a first individual, the first individual having a previously verified personal identity; assigning verification addresses on a block chain to the individuals, a given verification address including a public key and a private key, a first verification address being assigned to the first individual, the first verification address including a first public key and a first private key; and recording identifiers and biometric data associated with the individuals at corresponding verification addresses, the first identifier and first biometric data associated with the first individual being recorded at the first verification address.

The identity of the one or more individuals may be verifiable upon receiving matching biometric data and private keys, such that the personal identity of the first individual is verifiable upon receipt of (1) biometric data matching the first biometric data and (2) a private key matching the first private key.

Yet another aspect of the disclosure relates to a method for perform block chain-based multifactor personal identity verification using verification addresses. The method may be performed by one or more hardware processors configured by machine-readable instructions. The method may include receiving one or more identifiers in connection with one or more requests to verify an identity of one or more individuals, a first identifier being received in connection with a request to verify an identity of a first individual; extracting biometric data associated with the one or more individuals from corresponding verification addresses on a block chain, a given verification address including a public key and a private key, first biometric data associated with the first individual being extracted from a first verification address assigned to the first individual, the first verification address including a first public key and a first private key; and verifying the identity of the one or more individuals upon receiving matching biometric data and private keys, the personal identity of the first individual being verified upon receipt of (1) biometric data matching the first biometric data and (2) a private key matching the first private key.

These and other features, and characteristics of the present technology, as well as the methods of operation and functions of the related elements of structure and the combination of parts and economies of manufacture, will become more apparent upon consideration of the following description and the appended claims with reference to the accompanying drawings, all of which form a part of this specification, wherein like reference numerals designate corresponding parts in the various figures. It is to be expressly understood, however, that the drawings are for the purpose of illustration and description only and are not intended as a definition of the limits of the invention. As used in the specification and in the claims, the singular form of “a”, “an”, and “the” include plural referents unless the context clearly dictates otherwise.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 illustrates a system for providing block chain-based multifactor personal identity verification, in accordance with one or more implementations.

FIG. 2 illustrates a method for establishing verification addresses on a block chain in order to provide block chain-based multifactor personal identity verification, in accordance with one or more implementations.

FIG. 3 illustrates a method for performing block chain-based multifactor personal identity verification using verification addresses, in accordance with one or more implementations.

DETAILED DESCRIPTION

FIG. 1 illustrates a system **100** for providing block chain-based multifactor personal identity verification, in accordance with one or more implementations. In some implementations, system **100** may include one or more servers **102**. The server(s) **102** may be configured to communicate with one or more computing platforms **104** according to a client/server architecture, a peer-to-peer architec-

ture, and/or other architectures. The users may access system **100** via computing platform(s) **104**.

The server(s) **102** may be configured to execute machine-readable instructions **106**. The machine-readable instructions **106** may include one or more of an individual identifier component **108**, a verification address assignment component **110**, an address recordation component **112**, a user interface component **114**, a verification request component **116**, an information extraction component **118**, an identity verification component **120**, and/or other machine-readable instruction components.

The machine-readable instructions **106** may be executable to establish verification addresses on a block chain. Generally speaking, a block chain is a transaction database shared by some or all nodes participating in system **100**. Such participation may be based on the Bitcoin protocol, Ethereum protocol, and/or other protocols related to digital currencies and/or block chains. A full copy of the block chain contains every transaction ever executed in an associated digital currency. In addition to transactions, other information may be contained by the block chain, such as described further herein.

The block chain may be based on several blocks. A block may include a record that contains and confirms one or more waiting transactions. Periodically (e.g., roughly every one minute), a new block including transactions and/or other information may be appended to the block chain. In some implementations, a given block in the block chain contains a hash of the previous block. This may have the effect of creating a chain of blocks from a genesis block (i.e., the first block in the block chain) to a current block. The given block may be guaranteed to come chronologically after a previous block because the previous block's hash would otherwise not be known. The given block may be computationally impractical to modify once it is included in the block chain because every block after it would also have to be regenerated.

A given verification address may include a specific location on the block chain where certain information is stored. In some implementations, an individual verification address may be referred to as an "AtenVerify Address." Verification addresses are further described below in connection with verification address assignment component **110**.

The individual identifier component **108** may be configured to associated identifiers with individuals having previously verified personal identities. For example, a first identifier may be associated a first individual. The first individual may have a previously verified personal identity. Generally speaking, an identifier may include one or more of a number, an alphanumeric code, a username, and/or other information that can be linked to an individual. In some implementations, an individual identifier may be referred to as an "Aten ID."

In accordance with some implementations, an individual having a previously verified personal identity may have obtained the previously verified personal identity through a variety of approaches. For example, in some implementations the individual may be required to provide evidence of the individual's identity. Such evidence may include one or more of providing a copy of a government issued identification (e.g., passport and/or driver's license), providing a copy of mail received by the individual (e.g., a utility bill), evidence provided by a third party, and/or other evidence on an individual's identity. The evidence may be provided to an entity associated with server(s) **102**.

The verification address assignment component **110** may be configured to assign verification addresses on a block

chain to the individuals. A given verification address may include a public key and a private key. By way of example, a first verification address may be assigned to the first individual. The first verification address may include a first public key and a first private key.

Generally speaking, a public and private key-pair may be used for encryption and decryption according to one or more public key algorithms. By way of non-limiting example, a key pair may be used for digital signatures. Such a key pair may include a private key for signing and a public key for verification. The public key may be widely distributed, while the private key is kept secret (e.g., known only to its proprietor). The keys may be related mathematically, but calculating the private key from the public key is unfeasible.

In some implementations, verification address assignment component **110** may be configured such that private keys may be stored within computing platform(s) **104**. For example, the first private key may be stored within a computing platform **104** and/or other locations associated with the first individual. In accordance with some implementation, a private key may be stored in one or more of a "verify.dat" file, a SIM card, and/or other locations.

In some implementations, verification address assignment component **110** may be configured such that multiple verification addresses may be assigned to separate individuals. For example, in addition to the first verification address, a second verification address may be assigned to the first individual. One or more additional verification addresses may be assigned to the first individual, in accordance with one or more implementations.

The address recordation component **112** may be configured to record identifiers and biometric data associated with the individuals at corresponding verification addresses. For example, the first identifier and first biometric data associated with the first individual may be recorded at the first verification address. Recording information at a given verification address may include recording a hash or other encrypted representation of the information. In some implementations, different biometric data may be recorded at multiple verification addresses assigned to a single given individual. For example, in addition to the first identifier and the first biometric data associated with the first individual being recorded at the first verification address, the first identifier and second biometric data associated with the first individual may be recorded at a second verification address.

Generally speaking, biometric data may include metrics related to human characteristics. Biometric identifiers are distinctive, measurable characteristics that can be used to label and describe individuals. Biometric identifiers are typically include physiological characteristics, but may also include behavioral characteristics and/or other characteristics. Physiological characteristics may be related to the shape of an individual's body. Examples of physiological characteristics used as biometric data may include one or more of fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina, odor or scent, and/or other physiological characteristics. Behavioral characteristics may be related to a pattern of behavior of an individual. Examples of behavioral characteristics used as biometric data may include one or more of typing rhythm, gait, voice, and/or other behavioral characteristics.

The biometric data may include one or more of an image or other visual representation of a physiological characteristic, a recording of a behavioral characteristic, a template of a physiological characteristic and/or behavioral characteristic, and/or other biometric data. A template may include a synthesis of relevant features extracted from the source. A

template may include one or more of a vector describing features of a physiological characteristic and/or behavioral characteristic, a numerical representation of a physiological characteristic and/or behavioral characteristic, an image with particular properties, and/or other information.

Biometric data may be received via computing platforms **104** associated with the individuals. For example, biometric data associated with a first individual may be received via a first computing platform **104** associated with the first individual. The first computing platform **104** may include an input device (not depicted) configured to capture and/or record a physiological characteristic and/or behavioral characteristic of the first individual. Examples of such an input device may include one or more of a camera and/or other imaging device, a fingerprint scanner, a microphone, an accelerometer, and/or other input devices.

The user interface component **114** may be configured to provide an interface for presentation to individuals via associated computing platforms **104**. The interface may include a graphical user interface presented via individual computing platforms **104**. According to some implementations, the interface may be configured to allow a given individual to add or delete verification addresses assigned to the given individual so long as at least one verification address is assigned to the given individual.

In some implementations, user interface component **114** may be configured to access and/or manage one or more user profiles and/or user information associated with users of system **100**. The one or more user profiles and/or user information may include information stored by server(s) **102**, one or more of the computing platform(s) **104**, and/or other storage locations. The user profiles may include, for example, information identifying users (e.g., a username or handle, a number, an identifier, and/or other identifying information), security login information (e.g., a login code or password), system account information, subscription information, digital currency account information (e.g., related to currency held in credit for a user), relationship information (e.g., information related to relationships between users in system **100**), system usage information, demographic information associated with users, interaction history among users in the system **100**, information stated by users, purchase information of users, browsing history of users, a computing platform identification associated with a user, a phone number associated with a user, and/or other information related to users.

The machine-readable instructions **106** may be executable to perform block chain-based multifactor personal identity verification using the verification addresses.

The verification request component **116** may be configured to receive one or more identifiers in connection with one or more requests to verify an identity of one or more individuals. For example, the first identifier may be received in connection with a request to verify an identity of the first individual. Requests for identity verification may be provided in connection with and/or related to financial transactions, information exchanges, and/or other interactions. Requests may be received from other individuals and/or other third parties.

The information extraction component **118** may be configured to extract the biometric data associated with the one or more individuals from the corresponding verification addresses. For example, the first biometric data associated with the first individual may be extracted from the first verification address. Extracting information (e.g., biometric data) from a verification address may include decrypting information.

According to some implementations, information extraction component **118** may be configured such that, responsive to receiving the request to verify the identity of the first individual, a prompt may be provided to the first individual for biometric data matching the first biometric data and a private key matching the first private key. The prompt may be conveyed via a computing platform **104** associated with the first individual. The prompt may be conveyed via a graphical user interface and/or other user interface provided by the computing platform **104** associated with the first individual. The prompt may include an indication that is one or more of visual, audible, haptic, and/or other indications.

In some implementations, information extraction component **118** may be configured such that, responsive to receiving the request to verify the identity of the first individual, a prompt may be provided to a computing platform **104** associated with the first individual. The prompt may cause the computing platform **104** to automatically provide, to server(s) **102**, biometric data matching the first biometric data and/or a private key matching the first private key.

The identity verification component **120** may be configured to verify the identity of the one or more individuals upon, or in response to, receiving matching biometric data and private keys. For example, the personal identity of the first individual may be verified upon receipt of (1) biometric data matching the first biometric data and (2) a private key matching the first private key. Verifying the personal identity of the first individual may include comparing stored information with newly received information.

According to some implementations, identity verification component **120** may be configured such that the personal identity of the first individual may be verified upon receipt of (1) biometric data matching the first biometric data or the second biometric data and (2) a private key matching the first private key. Such implementations may provide so-called “M-of-N” signatures for identity verification where some subset of a larger set of identifying information is required.

In some implementations, identity verification component **120** may be configured such that the biometric data matching the first biometric data and the private key matching the first private key may be used to sign the verification of the personal identity of the first individual.

A cryptographic signature is a mathematical mechanism that allows someone to prove ownership. In the case of Bitcoin, a Bitcoin wallet and its private key(s) are linked by some mathematical magic. When your Bitcoin software signs a transaction with the appropriate private key, the whole network can see that the signature matches the bitcoins being spent. However, there is no way for the world to guess your private key to steal your hard-earned bitcoins.

In some implementations, at least one dedicated node performs the signing of the verification of the personal identity of the first individual. A given dedicated node may include one or more of the server(s) **102**. The given dedicated node may be a public node or a private node configured for creating new blocks and/or for signing verification.

In some implementations, server(s) **102**, computing platform(s) **104**, and/or external resources **122** may be operatively linked via one or more electronic communication links. For example, such electronic communication links may be established, at least in part, via a network such as the Internet and/or other networks. It will be appreciated that this is not intended to be limiting, and that the scope of this disclosure includes implementations in which server(s) **102**,

computing platform(s) **104**, and/or external resources **122** may be operatively linked via some other communication media.

A given computing platform **104** may include one or more processors configured to execute machine-readable instructions. The machine-readable instructions may be configured to enable an expert or user associated with the given computing platform **104** to interface with system **100** and/or external resources **122**, and/or provide other functionality attributed herein to computing platform(s) **104**. By way of non-limiting example, the given computing platform **104** may include one or more of a desktop computer, a laptop computer, a handheld computer, a tablet computing platform, a NetBook, a Smartphone, a gaming console, and/or other computing platforms.

External resources **122** may include sources of information, hosts and/or providers of virtual environments outside of system **100**, external entities participating with system **100**, and/or other resources. In some implementations, some or all of the functionality attributed herein to external resources **100** may be provided by resources included in system **100**.

Server(s) **102** may include electronic storage **124**, one or more processors **126**, and/or other components. Server(s) **102** may include communication lines, or ports to enable the exchange of information with a network and/or other computing platforms. Illustration of server(s) **102** in FIG. 1 is not intended to be limiting. Server(s) **102** may include a plurality of hardware, software, and/or firmware components operating together to provide the functionality attributed herein to server(s) **102**. For example, server(s) **102** may be implemented by a cloud of computing platforms operating together as server(s) **102**.

Electronic storage **124** may comprise non-transitory storage media that electronically stores information. The electronic storage media of electronic storage **124** may include one or both of system storage that is provided integrally (i.e., substantially non-removable) with server(s) **102** and/or removable storage that is removably connectable to server(s) **102** via, for example, a port (e.g., a USB port, a firewire port, etc.) or a drive (e.g., a disk drive, etc.). Electronic storage **124** may include one or more of optically readable storage media (e.g., optical disks, etc.), magnetically readable storage media (e.g., magnetic tape, magnetic hard drive, floppy drive, etc.), electrical charge-based storage media (e.g., EEPROM, RAM, etc.), solid-state storage media (e.g., flash drive, etc.), and/or other electronically readable storage media. Electronic storage **124** may include one or more virtual storage resources (e.g., cloud storage, a virtual private network, and/or other virtual storage resources). Electronic storage **124** may store software algorithms, information determined by processor(s) **126**, information received from server(s) **102**, information received from computing platform(s) **104**, and/or other information that enables server(s) **102** to function as described herein.

Processor(s) **126** may be configured to provide information processing capabilities in server(s) **102**. As such, processor(s) **126** may include one or more of a digital processor, an analog processor, a digital circuit designed to process information, an analog circuit designed to process information, a state machine, and/or other mechanisms for electronically processing information. Although processor(s) **126** is shown in FIG. 1 as a single entity, this is for illustrative purposes only. In some implementations, processor(s) **126** may include a plurality of processing units. These processing units may be physically located within the same device, or processor(s) **126** may represent processing functionality

of a plurality of devices operating in coordination. The processor(s) **126** may be configured to execute machine-readable instruction components **108**, **110**, **112**, **114**, **116**, **118**, **120**, and/or other machine-readable instruction components. Processor(s) **126** may be configured to execute machine-readable instruction components **108**, **110**, **112**, **114**, **116**, **118**, **120**, and/or other machine-readable instruction components by software; hardware; firmware; some combination of software, hardware, and/or firmware; and/or other mechanisms for configuring processing capabilities on processor(s) **126**. As used herein, the term “machine-readable instruction component” may refer to any component or set of components that perform the functionality attributed to the machine-readable instruction component. This may include one or more physical processors during execution of processor readable instructions, the processor readable instructions, circuitry, hardware, storage media, or any other components.

It should be appreciated that although machine-readable instruction components **108**, **110**, **112**, **114**, **116**, **118**, and **120** are illustrated in FIG. 1 as being implemented within a single processing unit, in implementations in which processor(s) **126** includes multiple processing units, one or more of machine-readable instruction components **108**, **110**, **112**, **114**, **116**, **118**, and/or **120** may be implemented remotely from the other machine-readable instruction components. The description of the functionality provided by the different machine-readable instruction components **108**, **110**, **112**, **114**, **116**, **118**, and/or **120** described below is for illustrative purposes, and is not intended to be limiting, as any of machine-readable instruction components **108**, **110**, **112**, **114**, **116**, **118**, and/or **120** may provide more or less functionality than is described. For example, one or more of machine-readable instruction components **108**, **110**, **112**, **114**, **116**, **118**, and/or **120** may be eliminated, and some or all of its functionality may be provided by other ones of machine-readable instruction components **108**, **110**, **112**, **114**, **116**, **118**, and/or **120**. As another example, processor(s) **126** may be configured to execute one or more additional machine-readable instruction components that may perform some or all of the functionality attributed below to one of machine-readable instruction components **108**, **110**, **112**, **114**, **116**, **118**, and/or **120**.

FIG. 2 illustrates a method **200** for establishing verification addresses on a block chain in order to provide block chain-based multifactor personal identity verification, in accordance with one or more implementations. The operations of method **200** presented below are intended to be illustrative. In some implementations, method **200** may be accomplished with one or more additional operations not described, and/or without one or more of the operations discussed. Additionally, the order in which the operations of method **200** are illustrated in FIG. 2 and described below is not intended to be limiting.

In some implementations, one or more operations of method **200** may be implemented in one or more processing devices (e.g., a digital processor, an analog processor, a digital circuit designed to process information, an analog circuit designed to process information, a state machine, and/or other mechanisms for electronically processing information). The one or more processing devices may include one or more devices executing some or all of the operations of method **200** in response to instructions stored electronically on an electronic storage medium. The one or more processing devices may include one or more devices con-

figured through hardware, firmware, and/or software to be specifically designed for execution of one or more of the operations of method **200**.

At an operation **202**, identifiers may be associated with individuals having previously verified personal identities. A first identifier may be associated a first individual. The first individual may have a previously verified personal identity. Operation **202** may be performed by one or more hardware processors configured to execute a machine-readable instruction component that is the same as or similar to individual identifier component **108** (as described in connection with FIG. 1), in accordance with one or more implementations.

At an operation **204**, verification addresses on a block chain may be assigned to the individuals. A given verification address may include a public key and a private key. A first verification address may be assigned to the first individual. The first verification address may include a first public key and a first private key. Operation **204** may be performed by one or more hardware processors configured to execute a machine-readable instruction component that is the same as or similar to verification address assignment component **110** (as described in connection with FIG. 1), in accordance with one or more implementations.

At an operation **206**, identifiers and biometric data associated with the individuals may be recorded at corresponding verification addresses. The first identifier and first biometric data associated with the first individual may be recorded at the first verification address. The identity of the one or more individuals may be verifiable upon, or in response to, receiving matching biometric data and private keys. The personal identity of the first individual may be verifiable upon, or in response to, receipt of (1) biometric data matching the first biometric data and (2) a private key matching the first private key. Operation **206** may be performed by one or more hardware processors configured to execute a machine-readable instruction component that is the same as or similar to address recordation component **112** (as described in connection with FIG. 1), in accordance with one or more implementations.

FIG. 3 illustrates a method **300** for performing block chain-based multifactor personal identity verification using verification addresses, in accordance with one or more implementations. The operations of method **300** presented below are intended to be illustrative. In some implementations, method **300** may be accomplished with one or more additional operations not described, and/or without one or more of the operations discussed. Additionally, the order in which the operations of method **300** are illustrated in FIG. 3 and described below is not intended to be limiting.

In some implementations, method **300** may be implemented in one or more processing devices (e.g., a digital processor, an analog processor, a digital circuit designed to process information, an analog circuit designed to process information, a state machine, and/or other mechanisms for electronically processing information). The one or more processing devices may include one or more devices executing some or all of the operations of method **300** in response to instructions stored electronically on an electronic storage medium. The one or more processing devices may include one or more devices configured through hardware, firmware, and/or software to be specifically designed for execution of one or more of the operations of method **300**.

At an operation **302**, one or more identifiers may be received in connection with one or more requests to verify an identity of one or more individuals. A first identifier may be received in connection with a request to verify an identity

of a first individual. Operation **302** may be performed by one or more hardware processors configured to execute a machine-readable instruction component that is the same as or similar to verification request component **116** (as described in connection with FIG. 1), in accordance with one or more implementations.

At an operation **304**, biometric data associated with the one or more individuals may be extracted from corresponding verification addresses on a block chain. A given verification address may include a public key and a private key. First biometric data associated with the first individual may be extracted from a first verification address assigned to the first individual. The first verification address may include a first public key and a first private key. Operation **304** may be performed by one or more hardware processors configured to execute a machine-readable instruction component that is the same as or similar to information extraction component **118** (as described in connection with FIG. 1), in accordance with one or more implementations.

At an operation **306**, the identity of the one or more individuals may be verified upon, or in response to, receiving matching biometric data and private keys. The personal identity of the first individual may be verified upon, or in response to, receipt of (1) biometric data matching the first biometric data and (2) a private key matching the first private key. Operation **306** may be performed by one or more hardware processors configured to execute a machine-readable instruction component that is the same as or similar to identity verification component **120** (as described in connection with FIG. 1), in accordance with one or more implementations.

Exemplary implementations may facilitate storing personal data on the block chain. The personal data may be stored on the block chain in an encrypted way. A person may be identified at the block chain level with one or more of a private key, a finger print, a finger print hash, an eye retina, an eye retina hash, and/or other unique information. The data stored may include or relate to one or more of a passport, an identification card, extracted passport information, a driver's license, extracted driver's license information, finger print, eye retina, and/or other information. According to some implementations, if some of the data is changed, a new record may be created for that person in the block chain. That is, all changes are added as new records. The old record will always be stored on the block chain. Generally speaking, all records on the block chain are stored forever and cannot be removed. More than one copy of the block chain will exist to ensure the records are not manipulated.

Exemplary implementations may facilitate access to personal data. There may be multiple access levels for the personal data in the block chain. Access controls may be granted on public/private key pairs levels. Examples of access levels may include one or more of Super Admin (full access to block chain), Authorities-country level (full read-only access), Authorities-state/local level (limited read-only access), Police and other services including Emergency (access to certain personal data by Finger Print/Eye retina of that person only), Participating Merchants (limited access), and/or other access levels.

Exemplary implementations may facilitate verification check. There may be multiple levels for how it is possible to check verification. For example, some implementations may ensure a person has a record at "Company" but no personal data is provided. Some implementations may ensure a person has a record at Company and get very basic personal information such as Full Name, DOB, Gender, and/or other

basic information. Some implementations may ensure a person has a record at Company and get all personal data.

Although the present technology has been described in detail for the purpose of illustration based on what is currently considered to be the most practical and preferred implementations, it is to be understood that such detail is solely for that purpose and that the technology is not limited to the disclosed implementations, but, on the contrary, is intended to cover modifications and equivalent arrangements that are within the spirit and scope of the appended claims. For example, it is to be understood that the present technology contemplates that, to the extent possible, one or more features of any implementation can be combined with one or more features of any other implementation.

What is claimed is:

1. A system for providing blockchain-based multifactor personal identity verification, the system comprising:

one or more computer-readable storage media configured to store a blockchain;

a server-side computer system comprising one or more processors programmed to execute computer program instructions that, when executed, cause the server-side computer system to:

assign a verification address associated with the blockchain to an individual, the individual having a previously verified personal identity;

store, at the one or more computer-readable storage media, an identifier of the individual and a biometric hash of the individual in association with the verification address associated with the blockchain, wherein the biometric hash is a hash of biometric data of the individual, and

wherein each of the identifier, the biometric hash, and the verification address are different from one another and different from private and public keys from which the verification address was derived;

obtain, from a client-side device, the identifier and the biometric data in connection with a request to verify the individual's identity, the request indicating the verification address associated with the blockchain; obtain the stored identifier and the stored biometric hash using the verification address indicated in the request; and

sign verification of the individual's identity responsive to a determination that the identifier of the request and the biometric data of the request match the stored identifier and the stored biometric hash.

2. The system of claim 1, wherein the server-side computer system is caused to:

sign, using the private key from which the verification address was derived, the verification of the individual's identity responsive to the determination that the identifier of the request and the biometric data of the request match the stored identifier and the stored biometric hash.

3. The system of claim 2, wherein the server-side computer system is caused to:

store, at the one or more computer-readable storage media, the private key in association with the verification address associated with the blockchain;

obtain, from the client-side device, the private key in connection with the request to verify the individual's identity;

obtain the stored private key using the verification address indicated in the request; and

sign, using the private key, the verification of the individual's identity responsive to a determination that the

identifier of the request, the biometric data of the request, and the private key of the request match the stored identifier, the stored biometric hash, and the stored private key.

4. The system of claim 3, wherein the private key is also stored on the client-side device, and wherein the client-side device is a user device of the individual.

5. The system of claim 1, wherein the server-side computer system is caused to:

assign another verification address associated with the blockchain to the individual;

store, at the one or more computer-readable storage media, another biometric hash of the individual in association with the other verification address associated with the blockchain, the other biometric hash being a hash of other biometric data of the individual; obtain, from the client-side device, the other biometric data in connection with the request to verify the individual's identity, the request further indicating the other verification address associated with the blockchain;

obtain the stored other biometric hash using the other verification address indicated in the request; and sign the verification of the individual's identity responsive to a determination that the identifier of the request, the biometric data of the request, the other biometric data of the request match the stored identifier, the stored biometric hash, and the stored other biometric hash.

6. The system of claim 5, wherein the server-side computer system is caused to:

obtain, via a user interface, a user-initiated command to add the other verification address as an address of the blockchain for the individual; and

assign the other verification address associated with the blockchain to the individual based on the user-initiated command.

7. The system of claim 5, wherein the server-side computer system is caused to:

obtain, via a user interface, a user-initiated command to remove the other verification address as an address of the blockchain for the individual; and

de-associate the other verification address associated with the blockchain from the individual based on the user-initiated command.

8. The system of claim 1, wherein the server-side computer system is caused to:

provide a first user, different than the individual, access to data stored at the one or more computer-readable storage media in association with the verification address associated with the blockchain, the first user being provided access to the stored data based on verification that the first user has a first private key, the first private key being different the private key from which the verification address was derived; and denying a second user, different than the individual, access to the stored data based on verification that the second user has a second private key.

9. The system of claim 1, wherein the biometric data comprises an image, a recording, or a template.

10. The system of claim 1, wherein the biometric data is related to a fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina, odor, gait, or voice.

11. A method of providing blockchain-based multifactor personal identity verification, the method being implemented by a server-side computer system comprising one or

13

more processors executing computer program instructions that, when executed, perform the method, the method comprising:

storing, by the server-side computer system, a blockchain at one or more computer-readable storage media of the server-side computer system;

assigning, by the server-side computer system, a verification address associated with the blockchain to an individual, the individual having a previously verified personal identity;

storing, by the server-side computer system, at the one or more computer-readable storage media, an identifier of the individual and a biometric hash of the individual in association with the verification address associated with the blockchain,

wherein the biometric hash is a hash of biometric data of the individual, and

wherein each of the identifier, the biometric hash, and the verification address are different from one another and different from private and public keys from which the verification address was derived;

obtaining, by the server-side computer system, from a client-side device, the identifier and the biometric data in connection with a request to verify the individual's identity, the request indicating the verification address associated with the blockchain;

obtaining, by the server-side computer system, the stored identifier and the stored biometric hash using the verification address indicated in the request; and

assigning, by the server-side computer system, verification of the individual's identity responsive to a determination that the identifier of the request and the biometric data of the request match the stored identifier and the stored biometric hash.

12. The method of claim 11, comprising:

signing, by the server-side computer system, using the private key from which the verification address was derived, the verification of the individual's identity responsive to the determination that the identifier of the request and the biometric data of the request match the stored identifier and the stored biometric hash.

13. The method of claim 12, comprising:

storing, by the server-side computer system, at the one or more computer-readable storage media, the private key in association with the verification address associated with the blockchain;

obtaining, by the server-side computer system, from the client-side device, the private key in connection with the request to verify the individual's identity;

obtaining the stored private key using the verification address indicated in the request; and

signing, by the server-side computer system, using the private key, the verification of the individual's identity responsive to a determination that the identifier of the request, the biometric data of the request, and the private key of the request match the stored identifier, the stored biometric hash, and the stored private key.

14. The method of claim 11, comprising:

assigning, by the server-side computer system, another verification address associated with the blockchain to the individual;

storing, by the server-side computer system, at the one or more computer-readable storage media, another biometric hash of the individual in association with the other verification address associated with the blockchain, the other biometric hash being a hash of other biometric data of the individual;

14

obtaining, by the server-side computer system, from the client-side device, the other biometric data in connection with the request to verify the individual's identity, the request further indicating the other verification address associated with the blockchain;

obtaining, by the server-side computer system, the stored other biometric hash using the other verification address indicated in the request; and

signing, by the server-side computer system, the verification of the individual's identity responsive to a determination that the identifier of the request, the biometric data of the request, the other biometric data of the request match the stored identifier, the stored biometric hash, and the stored other biometric hash.

15. The method of claim 14, comprising:

obtaining, by the server-side computer system, via a user interface, a user-initiated command to add the other verification address as an address of the blockchain for the individual; and

assigning, by the server-side computer system, the other verification address associated with the blockchain to the individual based on the user-initiated command.

16. The method of claim 14, comprising:

obtaining, by the server-side computer system, via a user interface, a user-initiated command to remove the other verification address as an address of the blockchain for the individual; and

de-associating, by the server-side computer system, the other verification address associated with the blockchain from the individual based on the user-initiated command.

17. The method of claim 11, comprising:

providing, by the server-side computer system, a first user, different than the individual, access to data stored at the one or more computer-readable storage media in association with the verification address associated with the blockchain, the first user being provided access to the stored data based on verification that the first user has a first private key, the first private key being different the private key from which the verification address was derived; and

denying, by the server-side computer system, a second user, different than the individual, access to the stored data based on verification that the second user has a second private key.

18. The method of claim 11, wherein the biometric data comprises an image, a recording, or a template.

19. The method of claim 11, wherein the biometric data is related to a fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina, odor, gait, or voice.

20. A system for providing blockchain-based multifactor personal identity verification, the system comprising:

one or more computer-readable storage media configured to store a blockchain;

a server-side computer system comprising one or more processors programmed to execute computer program instructions that, when executed, cause the server-side computer system to:

assign multiple verification addresses of the blockchain to the individual, the individual having a previously verified personal identity, the multiple verification addresses include a first verification address associated with the blockchain and a second verification address associated with the blockchain;

store, at the one or more computer-readable storage media, (i) an identifier of the individual and a first

15

biometric hash of the individual in association with the first verification address associated with the blockchain and (ii) a second biometric hash of the individual in association with the second verification address associated with the blockchain, 5

wherein the first biometric hash is a hash of first biometric data of the individual, and the second biometric hash is a hash of second biometric data of the individual, and

wherein each of the identifier, the first biometric hash, the second biometric hash, the first verification address, and the second verification address are different from one another, different from first private and public keys from which the first verification address was derived, and different from 10

second private and public keys from which the second verification address was derived;

obtain, from a client-side device, the identifier, the first biometric data, and the second biometric data in connection with a request to verify the individual's identity, the request indicating the first verification address associated with the blockchain and the second verification address associated with the blockchain; 20

obtain (i) the stored identifier and the stored first biometric hash using the first verification address 25

16

indicated in the request and (ii) the stored second biometric hash using the second verification address indicated in the request; and

sign, using the private key from which the first verification address was derived, verification of the individual's identity responsive to a determination that the identifier of the request, the first biometric data of the request, and the second biometric data of the request match the stored identifier, the stored first biometric hash, and the stored second biometric hash;

provide a first user, different than the individual, access to data stored at the one or more computer-readable storage media in association with the first verification address associated with the blockchain, the first user being provided access to the stored data based on verification that the first user has a first private key, the first private key being different the private key from which the first verification address was derived and different from the private key from which the second verification address was derived; and

deny a second user, different than the individual, access to the stored data based on verification that the second user has a second private key.

* * * * *



OFICINA DE PATENTES Y MARCAS DE ESTADOS UNIDOS

DEPARTAMENTO DE COMERCIO DE
ESTADOS UNIDOS
Oficina de Patentes y Marcas de Estados Unidos
Domicilio: COMISIONADO DE PATENTES
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

SOLICITUD N°	FECHA DE CONCESIÓN	PATENTE N°	N° DE EXPEDIENTE DEL ABOGADO	N° DE CONFIRMACIÓN
15/083.241	29/05/2018	9985964	17-10153	5060
36212	7590	05/09/2018		
HOFFMAN PATENT GROUP 28494 WESTINGHOUSE PLACE SUITE 204 VALENCIA, CA 91355				

NOTIFICACIÓN DE CONCESIÓN

El número de patente y la fecha de concesión proyectados se especifican arriba.

Determinación del Ajuste del Plazo de Patente según 35 U.S.C. 154 (b)

(solicitud presentada el 29 de mayo de 2000, o después)

El Ajuste del Plazo de Patente es de 143 día(s). Cualquier patente que se conceda a la solicitud identificada arriba incluirá una indicación del ajuste en la primera página.

Si se presentó una Solicitud de Seguimiento Continuo (CPA) en la solicitud identificada arriba, la fecha de presentación que determina el Ajuste del Plazo de Patente es la fecha de presentación de la CPA más reciente.

El Solicitante podrá obtener información más detallada accediendo a la página WEB de Recuperación de Información sobre Solicitudes de Patentes (Patent Application Information Retrieval (PAIR)) (<http://pair.uspto.gov>).

Cualquier pregunta relacionada con la determinación del Ajuste o la Extensión del Plazo de Patente debe dirigirse a la Oficina de la Administración Legal de Patentes al (571)-272-7702. Las preguntas relacionadas con los pagos de aranceles por concesión y publicación deben dirigirse a la Unidad de Asistencia sobre Solicitudes (Application Assistance Unit (AAU)) de la Oficina de Gestión de Datos (ODM) al (571)-272-4200.

SOLICITANTE(S) (Sírvese ver página WEB de PAIR <http://pair.uspto.gov> para conocer solicitantes adicionales):

Marcus Andrade, Fernley, NV;

BLACK GOLD COIN, INC., Las Vegas, NV;

Los Estados Unidos representan el mercado más grande, más dinámico en el mundo y es una ubicación sin paralelo para inversión comercial, innovación y comercialización de nuevas tecnologías. Los EE. UU. ofrecen recursos y ventajas tremendos para aquellos que invierten y fabrican productos aquí. A través de SelectUSA, nuestra nación trabaja para alentar y facilitar la inversión comercial. Para conocer más sobre por qué los EE. UU. son el mejor país en el mundo para desarrollar tecnología, fabricar productos y hacer crecer su comercio, visite SelectUSA.gov.



OFICINA DE PATENTES Y MARCAS DE ESTADOS UNIDOS

DEPARTAMENTO DE COMERCIO DE ESTADOS
UNIDOS
Oficina de Patentes y Marcas de Estados Unidos
Dirección: COMISIONADO DE PATENTES
P.O. Box 1450
Alexandria, Virginia 22313-1450

NOTIFICACIÓN DE CONCESIÓN Y ARANCEL(ES) ADEUDADO(S)

909 7590 18/04/2018
Pillsbury Winthrop Shaw Pittman, LLP PO
Box 10500 McLean, VIRGINIA 22102
UNITED STATES OF AMERICA

GOODCHILD, WILLIAM J

UNIDAD DEL ARTE NÚMERO DE DOCUMENTO

2433

FECHA DE ENVÍO: 18/04/2018

Nº DE SOLICITUD	FECHA DE PRESENTACIÓN	PRIMER INVENTOR NOMBRADO	Nº DE EXP. DEL ABOGADO	Nº DE CONFIRMACIÓN
-----------------	-----------------------	--------------------------	------------------------	--------------------

15/083.241

03/28/2016

Marcus Andrade

038918-0444639

5060

TÍTULO DE LA
INVENCIÓN :
VERIFICACIÓN

SISTEMAS Y MÉTODOS PARA PROPORCIONAR IDENTIDAD PERSONAL MULTIFACTORIAL BASADA EN CADENA DE BLOQUES

TIPO DE SOLIC.	ESTADO DE ENTIDAD	ARANCEL DE CONCESIÓN	ARANCEL DE PUBLICACIÓN	ARANCEL DE CONCESIÓN ABONADO	TOTAL ARANCEL(ES) ADEUDADO(S)	FECHA DE VENCIMIENTO
----------------	-------------------	----------------------	------------------------	------------------------------	-------------------------------	----------------------

no provisional

PEQUEÑA

\$500

\$0.00

\$0.00

\$500

18/07/2018

LA SOLICITUD IDENTIFICADA ARRIBA SE HA EXAMINADO Y ESTÁ AUTORIZADA PARA CONCEDERSE COMO PATENTE. EL SEGUIMIENTO SOBRE LOS MÉRITOS ESTÁ CERRADO. ESTA NOTIFICACIÓN DE CONCESIÓN NO ES LA CONCESIÓN DE LOS DERECHOS DE LA PATENTE. ESTA SOLICITUD ESTÁ SUJETA AL RETIRO DE EMISIÓN A INICIATIVA DE LA OFICINA O TRAS LA PETICIÓN DEL SOLICITANTE. VÉASE 37 CFR 1.313 Y MPEP 1308.

EL ARANCEL DE CONCESIÓN Y DE PUBLICACIÓN (SI SE REQUIEREN) DEBEN ABONARSE DENTRO DE LOS TRES MESES DESDE LA FECHA DE ENVÍO DE ESTA NOTIFICACIÓN O ESTA SOLICITUD SE CONSIDERARÁ ABANDONADA. ESTE PERÍODO FIJADO POR LEY NO PUEDE EXTENDERSE. VÉASE 35 U.S.C. 151. EL ARANCEL DE CONCESIÓN ADEUDADO INDICADO ARRIBA NO REFLEJA UN CRÉDITO POR NINGÚN ARANCEL DE CONCESIÓN ABONADO PREVIAMENTE EN ESTA SOLICITUD. SI ANTERIORMENTE SE HA ABONADO UN ARANCEL DE CONCESIÓN EN ESTA SOLICITUD (COMO SE MUESTRA ARRIBA), LA DEVOLUCIÓN DE LA PARTE B DE ESTE FORMULARIO SE CONSIDERARÁ UNA SOLICITUD PARA VOLVER A APLICAR EL ARANCEL DE CONCESIÓN PREVIAMENTE PAGADO AL ARANCEL DE CONCESIÓN ADEUDADO AHORA.

CÓMO RESPONDER ESTA NOTIFICACIÓN:

I. Revise el ESTADO DE ENTIDAD que aparece arriba. Si el ESTADO DE ENTIDAD se muestra como PEQUEÑA O MICRO, verifique si aún aplica esa categoría para ese estado de entidad.

Si el ESTADO DE ENTIDAD es el mismo que aparece arriba, abone el/los ARANCEL(ES) TOTALES ADEUDADOS que se muestran arriba.

Si el ESTADO DE ENTIDAD es distinto a lo que aparece arriba, en la PARTE B - TRANSMISIÓN DE ARANCEL(ES), complete la sección número 5 titulada "Cambio en el Estado de la Entidad (del estado que se indica arriba)".

Para los fines de esta notificación, los aranceles de pequeña entidad son 1/2 de la cantidad de los aranceles sin descuento, y los aranceles de micro entidad son de 1/2 de la cantidad de los aranceles de pequeña entidad.

II. La PARTE B - TRANSMISIÓN DE ARANCEL(ES), o su equivalente, debe completarse y devolverse a la Oficina de Patentes y Marcas de Estados Unidos (USPTO) con su ARANCEL DE CONCESIÓN y ARANCEL DE PUBLICACIÓN (si se requiere). Si carga su(s) arancel(es) a su cuenta de depósito, la sección "4b" de la Parte B - Transmisión de Arancel(es) debe completarse y debe presentarse una copia extra de formulario. Si se presenta un equivalente de la Parte B, debe realizarse claramente una solicitud de volver a aplicar el arancel de concesión previamente pagado, y pueden ocurrir demoras en el procesamiento debido a la dificultad de reconocer el documento como un equivalente de la Parte B.

III. Todas las comunicaciones referidas a esta solicitud deben suministrar el número de solicitud. Sírvase dirigir todas las comunicaciones previas a la concesión a Mail Stop ISSUE FEE a menos que se le indique de otro modo.

RECORDATORIO IMPORTANTE: La concesión de patentes de utilidad sobre solicitudes presentadas a partir del 12 de diciembre de 1980 puede requerir el pago de aranceles de mantenimiento. Es responsabilidad de quien presenta la patente asegurar el pago oportuno de los aranceles de mantenimiento cuando se venzan.

PARTE B - TRANSMISIÓN DE ARANCEL(ES)

Completar y enviar este formulario, junto con los aranceles aplicables, a: **Correo Mail Stop ISSUE FEE**
Comisionado de Patentes
P.O. Box 1450
Alexandria, Virginia 22313-1450
o Fax (571)-273-2885

INSTRUCCIONES: Este formulario debe usarse para transmitir el ARANCEL DE CONCESIÓN y el ARANCEL DE PUBLICACIÓN (si se requiere). Los bloques 1 a 5 deben completarse donde corresponda. Toda correspondencia adicional que incluya aranceles de la Patente, ordenes de anticipo y notificaciones de mantenimiento se enviará a la dirección postal vigente a menos que se corrija abajo o se indique de otro modo en el Bloque 1, mediante (a) especificación de una nueva dirección postal; y/o (b) indicación de una "DIRECCIÓN DE ARANCELES" separada para notificaciones sobre el arancel de mantenimiento.

DIRECCIÓN POSTAL ACTUAL (Nota: Usar el Bloque 1 para cualquier cambio de dirección)

Nota: Un certificado de envío postal solo puede usarse para envíos locales de Transmisión de Arancel(es). Este certificado no puede usarse para ningún otro documento adjunto. Cada documento adicional, tal como una cesión o dibujo formal, debe tener su propio certificado de envío o transmisión.

909 7590 18/04/2018
Pillsbury Winthrop Shaw Pittman, LLP PO
Box 10500 McLean, VIRGINIA 22102
UNITED STATES OF AMERICA

Certificado de Envío Postal o Transmisión
Certifico en este acto que esta Transmisión de Arancel(es) se deposita en el Servicio Postal Norteamericano con franqueo suficiente para envío de primera clase en un sobre dirigido a la dirección Mail Stop ISSUE FEE que antecede, o se transmite por fax a la USPTO al (571) 273-2885, en la fecha indicada más abajo.

(Nombre del Depositante)

(Firma)

(Date)

Nº DE SOLICITUD	FECHA DE PRESENTACIÓN	PRIMER INVENTOR NOMBRADO	Nº DE EXP. DEL ABOGADO	Nº DE CONFIRMACIÓN
15/083.241	28/03/2016	Marcus Andrade	038918-0444639	5060

TÍTULO DE LA INVENCIÓN: SISTEMAS Y MÉTODOS PARA PROPORCIONAR IDENTIDAD PERSONAL MULTIFACTORIAL BASADA EN CADENA DE BLOQUES
VERIFICACIÓN

TIPO DE SOLICITUD	ESTADO DE ENTIDAD	ARANCEL DE CONCESIÓN VENCIDO	ARANCEL DE PUBLICACIÓN VENCIDO	ARANCEL DE CONCESIÓN PAGADO	TOTAL ARANCEL ADEUDADO	FECHA DE VENCIMIENTO
no provisional	PEQUEÑA	\$500	\$0.00	\$0.00	\$500	18/07/2018
EXAMINADOR	UNIDAD DEL ARTE	CLASE - SUB-CLASE				
GOODCHILD, WILLIAM J	2433	726-006000				

1. Cambio de domicilio postal o indicación de "Domicilio de Aranceles" (37 CFR 1.363).
☐ Formulario de Cambio de domicilio postal (o Cambio de Domicilio de Correspondencia PTO/SB/122) adjunto.

2. Para imprimir en la primera página de la patente, mencionar
(1) Los nombres de hasta 3 apoderados o agentes registrados 1
O, alternativamente, 2
(2) El nombre de una sola empresa (que tiene como miembro un apoderado o agente registrado) y los nombres de hasta 2 apoderados o agentes de patentes registrados. Si no se menciona nombre, no se imprimirá ningún nombre.

☐ Indicación del "Domicilio de Aranceles" (o Form. de Indicación de "Domicilio de Aranceles PTO/SB/47; Rev 03-02 o más reciente) adjunto. **Se requiere el uso de un Número de Cliente.**

3. NOMBRE Y DATOS DE RESIDENCIA DEL CESIONARIO A IMPRIMIR EN LA PATENTE (imprimir o escribir a máquina)
SE DEBE OBSERVAR QUE: A menos que se identifique un cesionario más abajo, no aparecerán datos del cesionario en la patente. Si se identifica un cesionario abajo, el documento se ha presentado como registro como se establece en 37 CFR 3.11. La compleción de este formulario NO sustituye la presentación de una cesión.
(A) NOMBRE DEL CESIONARIO (B) RESIDENCIA: (CIUDAD y ESTADO O PAÍS)

Por favor tildar la categoría o las categorías apropiadas del cesionario (no se imprimirá en la patente): ☐ Individuo ☐ Sociedad u otra entidad de grupo privado ☐ Gobierno

4a. Se presentará(n) el(los) siguiente(s) aranceles:

4b. Pago de Arancel(es): **(Por favor volver a aplicar primero cualquier arancel previamente abonado como se muestra arriba)**

- ☐ Arancel de Concesión
☐ Arancel de Publicación (No se permite descuento de pequeña entidad)
☐ Orden de anticipo - # Copias
- ☐ Se adjunta cheque.
☐ Pago por tarjeta de crédito. Se adjunta Formulario PTO-2038.
☐ Se autoriza al director a cargar el(los) arancel(es) requerido, cualquier deficiencia o acreditar cualquier pago extra, a la Cuenta de Depósito Número (adjuntar copia extra de este formulario).

5. Cambio en el Estado de Entidad (del estado indicado arriba)

- ☐ El solicitante certifica estado de micro entidad. Ver 37 CFR 1.29
- ☐ El solicitante justifica estado de pequeña entidad. Ver 37 CFR 1.27
- ☐ El solicitante cambia a estado de arancel regular sin descuento.

NOTA: Sin certificación válida del Estado de Micro Entidad (ver forms. PTO/SB/15A y 15B), no se aceptará pago por la suma de micro entidad a riesgo de abandono de la solicitud.

NOTA: Si la solicitud anteriormente fue por un estado de micro entidad, el tildado de este casillero se considerará una notificación de la pérdida de capacidad como estado de micro entidad.

NOTA: El tildado de este casillero se considerará notificación de la capacidad como estado de pequeña o micro entidad, según corresponda.

NOTA: Este formulario debe firmarse de acuerdo con 37 CFR 1.31 y 1.33. Véase 37 CFR 1.4 para conocer los requerimientos de firma y certificaciones.

Firma Autorizada _____ Fecha _____

Nombre a máquina o impreso

Nº de Registro



OFICINA DE PATENTES Y MARCAS DE ESTADOS UNIDOS

DEPARTAMENTO DE COMERCIO DE ESTADOS UNIDOS

Oficina de Patentes y Marcas de Estados Unidos

Domicilio: COMISIONADO DE PATENTES

P.O. Box 1450

Alexandria, Virginia 22313-1450

www.uspto.gov

Nº DE SOLICITUD	FECHA DE PRESENTACIÓN	PRIMER INVENTOR NOMBRADO	Nº DE EXP. DEL ABOGADO	Nº DE CONFIRMACIÓN
15/083.241	28/03/2016	Marcus Andrade	038918-0444639	
909	7590	18/04/2018		
Pillsbury Winthrop Shaw Pittman, LLP PO Box 10500 McLean, VIRGINIA 22102 UNITED STATES OF AMERICA			EXAMINADOR GOODCHILD, WILLIAM J	
			UNIDAD DEL ARTE 2433	NÚMERO DE DOCUMENTO
FECHA DE ENVÍO: 18/4/2018				

Determinación del Ajuste del Plazo de Patente según 35 U.S.C. 154 (b) (Solicitudes presentadas a partir del 29 de mayo de 2000, inclusive)

La Oficina ha interrumpido la provisión del cálculo de Ajuste del Plazo de Patentes (por las siglas del inglés: Patent Term Adjustment (PTA)) con la Notificación de Concesión.

La Sección 1(h) (2) de la Ley de Correcciones Técnicas de AIA 35 U.S.C. 154(b) (3) (B) (i) se modificó para eliminar el requerimiento de que la Oficina proporcione una determinación del ajuste del plazo de patente con la notificación de concesión. Véase Revisiones al Ajuste del Plazo de Patentes, 78 Fed. Reg. 19416, 19417 (1 de abril de 2013). Por lo tanto, la Oficina ya no proporciona una determinación del ajuste del plazo de patente inicial con la notificación de concesión. La Oficina continuará suministrando una determinación del ajuste del plazo de patente con la Carta de Notificación de Concesión que se envía al solicitante aproximadamente tres semanas antes de la fecha de concesión de la patente, se incluirá el ajuste del plazo de patente sobre la misma. Cualquier solicitud de reconsideración de la determinación de ajuste del plazo de patente (o la reincorporación del ajuste del plazo de patente) seguirá el proceso definido en 37 CFR 1.705.

Cualquier consulta relacionada con la determinación del Ajuste o de la Extensión del Plazo de Patente debe dirigirse a la Administración Legal de la Oficina de Patentes al (571)-272-7702. Las preguntas relacionadas con los pagos de aranceles de concesión y publicación deben dirigirse al Centro de Atención al Cliente de la Oficina de Publicación de Patentes al 1-(888)-786-0101 o al (571)-272-4200.

***Notificación que requiere
juramento o declaración del
inventor***

Nº DE SOLICITUD 15/083.241	Solicitante(s) Marcus Andrade	
Examinador GOODCHILD, WILLIAM J	Unidad del arte 2433	

Esta notificación es un anexo a la Notificación de Concesión (PTOL-37), o a la Notificación de Concesión para una Solicitud de Diseño (PTOL-37D).

Aún no se ha presentado un juramento o una declaración del inventor, en cumplimiento con lo dispuesto en 37 CFR 1.63 o 1.64 ejecutado por o con respecto a cada inventor.

Un juramento o una declaración en cumplimiento con 37 CFR 1.63, o una declaración sustituta en cumplimiento con 37 CFR 1.64, ejecutados por, o con respecto a, cada inventor (para cualquier inventor para el cual no se haya presentado aún un juramento, una declaración o una declaración sustituta pertinente) DEBE presentarse no después de la fecha en la cual se abona el arancel de concesión. Véase 35 U.S.C. 115(f). La falta de cumplimiento en término generará el ABANDONO de esta solicitud.

No se ha recibido un juramento o una declaración de inventor debidamente ejecutados para el(los) siguiente(s) inventor(es):

Si el solicitante presentó previamente uno o más juramentos, declaraciones o declaraciones sustitutas, el solicitante puede haber recibido una notificación informativa respecto de las deficiencias encontradas:

INFORMAL ACTION PROBLEMS

- No se ha recibido un juramento o una declaración de inventor ejecutados apropiadamente para el(los) siguiente(s) inventor(es): **Marcus Andrade.**

El solicitante puede presentar el juramento o la declaración del inventor en cualquier momento antes del envío de la Notificación de Concesión y el Vencimiento de Cumplimiento y Ejecución, PTOL-85.

Las preguntas relacionadas con esta Notificación deben dirigirse a la Unidad de Asistencia sobre Solicitudes al 571-272-4200.

Autorización de la OMB y declaración de la PRA para PTOL-85 Parte B

La Ley de Reducción de Papelería (PRA) de 1995 requiere que las agencias Federales obtengan aprobación de la Oficina de Gestión y Presupuesto antes de solicitar muchos tipos de información del público. Cuando la OMB aprueba la solicitud de una agencia de recolectar información del público, la OMB (i) provee un Número de Control Válido y una fecha de vencimiento para que la agencia muestre en el documento que será utilizado para recolectar información y (ii) requiere que la agencia informe al público sobre la importancia legal del Número de Control de la OMB de acuerdo con 5 CFR 1320.5(b).

La información recolectada por PTOL-85 Parte B es un requerimiento según 37 CFR 1.311. Se requiere la información para obtener o mantener un beneficio del público que es presentar (y a través de la USPTO procesar) una solicitud. La confidencialidad se rige por 35 U.S.C. 122 y 37 CFR 1.14. Se estima que esta recolección toma 12 minutos para completarse, lo cual incluye reunir, preparar y presentar el formulario de solicitud completo ante la USPTO. El tiempo variará dependiendo de cada caso individual. Cualquier comentario sobre la cantidad de tiempo que le insume completar este formulario y/o las sugerencias para reducir esta carga, deben enviarse al Jefe de Funcionarios de Información, Oficina de Patentes y Marcas de EE. UU., Departamento de Comercio de EE. UU., P.O. Box 1450, Alexandria, Virginia 22313-1450. **NO ENVIAR ARANCELES NI FORMULARIOS COMPLETADOS A ESTA DIRECCIÓN. ENVIARLOS A:** Comisionado de Patentes, P.O. Box 1450, Alexandria, Virginia 22313-1450. De acuerdo con la Ley de Reducción de Papelería de 1995, ninguna persona está obligada a responder a una recolección de información a menos que se muestre un número de control válido de la OMB.

DECLARACIÓN DE LA LEY DE PRIVACIDAD

La **Ley de Privacidad de 1974 (P.L. 93-579)** requiere que se provea cierta información en relación con la presentación del formulario adjunto relacionado con una solicitud de patente o patente. De acuerdo con lo requerido por la Ley, le informamos que: (1) la autoridad general con respecto a la recopilación de esta información es U.S.C. 35 2(b)(2); (2) la presentación de la información es voluntaria; y (3) el propósito principal para el cual la Oficina de Patentes de los EE.UU. utilizará esta información es procesar y/o examinar la presentación de una solicitud de patente o patente. Si no se presentara la información requerida, existe la posibilidad de que a la Oficina de Patentes y Marcas no le sea posible procesar y/o examinar la presentación, lo cual puede tener como consecuencia la finalización de los procedimientos o el abandono de la solicitud o el vencimiento de la patente.

1. La información provista por el solicitante en el presente formulario está destinada normalmente a lo siguiente:
2. 1. La información del presente formulario recibirá tratamiento confidencial en la medida que lo permita la Ley de Libertad de Información (552 del U.S.C. 5) y Ley de Privacidad (552a del U.S.C. 5). Los registros provenientes del sistema del registro pueden ser revelados al Departamento de Justicia a fin de determinar si la revelación de estos registros es requerida por la Ley de Libertad de Información.
3. 2. Como procedimiento de rutina, es posible revelar un registro de este sistema de registros en el curso de la presentación de evidencia a una corte, magistrado o tribunal administrativo, incluyendo revelaciones al abogado oponente en el curso de las negociaciones.
4. 3. Como procedimiento de rutina, es posible revelar un registro de este sistema de registros a un Miembro de Congreso que presente una solicitud con referencia a un individuo al cual pertenecen los registros, cuando dicho individuo ha solicitado la colaboración del Miembro del Congreso con respecto al asunto al cual se refiere el registro.
5. 4. Como procedimiento de rutina, es posible revelar un registro de este sistema de registros a un contratista de una Agencia que necesite de tal información a fin de redactar un contrato. Las personas que reciben la información deberán cumplir los requerimientos de la Ley de Privacidad de 1974, según sus enmiendas, de acuerdo con el artículo 552a(m) del 5 U.S.C.
6. 5. Como procedimiento de rutina, es posible revelar a la Oficina de la Organización de la Propiedad Intelectual Mundial, una Solicitud Internacional presentada bajo el Tratado de Cooperación en Patentes que se encuentre en este sistema, de acuerdo con el Tratado de Cooperación.
7. 6. Como procedimiento de rutina, es posible revelar un registro de este sistema de registros a otra dependencia federal para revisión por motivos de Seguridad Nacional (181 U.S.C 35) y para revisión de acuerdo con la Ley de Energía Atómica (218 (c) U.S.C. 42).
8. 7. Como procedimiento de rutina, es posible revelar un registro de este sistema de registros al Administrador de Servicios Generales o la persona designada por el mismo, durante una inspección de los registros realizada por GSA como parte de la responsabilidad de la institución de recomendar mejoras en las prácticas de manejo de los registros y programas, de acuerdo con 2904 y 2906 del U.S.C. 44. Tales revelaciones se realizarán de acuerdo con las leyes de GSA que gobiernan la inspección de registros con dicho propósito y otras directivas pertinentes (es decir, GSA o Comercio). Tales revelaciones no serán utilizadas para efectuar resoluciones con respecto los individuos.
9. 8. Como procedimiento de rutina, es posible revelar un registro de este sistema de registros al público luego de la publicación de la solicitud de acuerdo con 122(b) del U.S.C. 35 o de la emisión de una patente de acuerdo con 151 del U.S.C. 35. Además, normalmente es posible revelar al público un registro, con las limitaciones impuestas por 1.14 del 37 CFR, si el registro fue presentado en una solicitud luego abandonada o cuya tramitación haya finalizado y que es mencionada como referencia por una solicitud publicada, una solicitud abierta a la inspección del público o una patente concedida.
9. Como procedimiento de rutina, es posible que se revele un registro de este sistema de registros a una entidad reguladora o judicial, federal o local si la USPTO considera que existe una violación o violación potencial de una ley o reglamento.

Notificación de Concesión

Nº DE SOLICITUD	Solicitante(s)	
15/083.241	Andrade, Marcus	
Examinador	Unidad del arte	Estado AIA
WILLIAM J GOODCHILD	2433	Sí

- La FECHA DE ENVÍO de esta comunicación aparece en la carátula con la dirección de correspondencia -

Siendo patentables todas las reivindicaciones, la TRAMITACIÓN SOBRE LOS MÉRITOS ESTÁ (O PERMANECE) CERRADA en esta solicitud.

Si no se incluye aquí (o se envió anteriormente), una Notificación de concesión (PTOL-85) u otra comunicación apropiada se enviará en su debido momento. **ESTA NOTIFICACIÓN DE CONCESIÓN NO ES UNA CONCESIÓN DEL DERECHO DE PATENTES.** Esta solicitud está sujeta a que se retire la concesión a iniciativa de la Oficina o a petición del solicitante. Véase 37 CFR 1.313 y MPEP 1308.

1. ☒ Esta comunicación es la respuesta a 19/12/2017.

☐ Una declaración(es)/declaración(es) jurada(s) según **37 CFR 1.130(b)** se presentó el _____.

2. ☐ El solicitante realizó una elección en respuesta a un requerimiento de restricción durante una entrevista el _____; el requerimiento de restricción y elección se han incorporado a esta acción.

3. ☒ La(s) reivindicaciones concedidas es/son 21-40. Como resultado de la(s) reivindicación(es) concedidas, puede ser elegible para el beneficio del programa de **Vía Rápida para la Prosecución de Patentes** en una oficina de propiedad intelectual participativa para la correspondiente solicitud. Para mayor información, remítase a

http://www.uspto.gov/patents/init_events/pph/index.jsp o envíe una consulta a PPHfeedback@uspto.gov.

4. ☐ Se acusa recibo de la reivindicación para una prioridad extranjera según lo dispuesto en 35 U.S.C. § 119(a)-(d) o (f).

Copias certificadas:

a) ☐ TODAS b) ☐ Algunas *c) ☐ Ninguna de:

1. ☐ Copias certificadas de los documentos de prioridad se han recibido

2. ☐ Copias certificadas de los documentos de prioridad se han recibido en la Solicitud N°. _____.

3. ☐ Copias de las copias certificadas de los documentos de prioridad se han recibido en esta solicitud en etapa nacional de la Oficina Internacional (Regla PCT 17.2(a)).

* Copias certificadas no recibidas: _____.

El solicitante tiene TRES MESES DESDE LA "FECHA DEL ENVÍO" de esta comunicación para presentar una respuesta que cumple con los requerimientos indicados abajo. La falta de cumplimiento oportuno generará el ABANDONO de esta solicitud.

ESTE PERÍODO DE TRES MESES NO TIENE PRÓRROGA.

5. ☐ Deben presentarse DIBUJOS CORREGIDOS (como "hojas de reemplazo").

☐ incluyendo los cambios requeridos por la Enmienda/Comentario del Examinador adjunto en la Vista del

Documento No./Datos de correo _____.

Los signos de identificación tales como el número de solicitud (ver 37 CFR 1.84(c)) deben escribirse en los dibujos en el anverso (no en el reverso) de cada hoja. La(s) hoja(s) de reemplazo debe etiquetarse como tales en el encabezado de acuerdo con 37 CFR 1.121(d).

6. ☐ Debe presentarse el DEPÓSITO DE y/o la INFORMACIÓN sobre el depósito de MATERIAL BIOLÓGICO. Observar el comentario del Examinador adjunto respecto del REQUERIMIENTO PARA DEPÓSITO DE MATERIAL BIOLÓGICO.

Anexo(s)

1. ☒ Notificación de Referencias citadas (PTO-892)

2. ☐ Declaraciones de Divulgación de Información (PTO/SB/08),

Nº de Doc./Fecha de envío _____.

3. ☐ Comentario del Examinador respecto del requerimiento para depósito de material biológico _____.

4. ☐ Resumen de la entrevista (PTO-413),

Nº de Doc./Fecha de envío..

5. ☐ Enmienda/Comentario del Examinador

6. ☐ Declaración del examinador de los motivos de la Concesión

7. ☐ Otros _____.

/William J. Goodchild/

Examinador Primario, Unidad del arte 2433

Unidad del arte: 2433

ACCIÓN DETALLADA

Notificación de Pre-AIA o Estado AIA

1. La presente solicitud, presentada el, o después del, 16 de marzo de 2013, está sometida a examen según el primer inventor para presentar las disposiciones de la AIA.

Respuesta a los argumentos

2. Los argumentos del solicitante, véase Comentarios, presentados el 19/12/2017, con respecto a las reivindicaciones 21 - 40 se han considerado de manera completa y son persuasivos. Las 102/103 objeciones se han retirado.

Tema susceptible de concesión

3. Se conceden las reivindicaciones 21-40.
4. Lo que sigue es una declaración del examinador de los motivos de concesión: las reivindicaciones independientes modificadas relacionadas con "donde cada uno del identificador, el resumen biométrico y la dirección de verificación son diferentes entre sí y son diferentes de las llaves privadas y públicas de la cual derivó la dirección de verificación;" y "obtener, de un dispositivo del cliente, los datos del identificador y biométricos en conexión con una solicitud de verificar la identidad del individuo, donde la solicitud indica la dirección de verificación de la cadena de bloqueo" no se encuentran dentro del arte previo. Cualquier comentario considerado necesario de parte del solicitante debe presentarse antes de que se realice el pago del arancel de concesión y, para evitar demoras en el procesamiento, preferentemente debe acompañar el arancel de concesión. Dichas presentaciones deben etiquetarse claramente como "Comentarios sobre la Declaración de los Motivos de Concesión."

Conclusión

5. Cualquier consulta relacionada con esta comunicación o con comunicaciones anteriores del examinador debe dirigirse a WILLIAM J GOODCHILD cuyo número de teléfono es (571)270-1589. El examinador puede contactarse normalmente de L. a V. de 8:00 a 16:30 hs.

Las entrevistas con el Examinador están a disposición por teléfono, en persona y por conferencia en video con el uso de una herramienta de colaboración basada en Internet proporcionada por la USPTO. Para programar una entrevista, se alienta al solicitante a usar la Solicitud de Entrevista Automática de la USPTO (Automated Interview Request (AIR)) en <http://www.uspto.gov/interviewpractice>.

Si los intentos por contactar al examinador son negativos, se puede comunicar con el supervisor del examinador, Jeff Pwu al 571-272-6798. El número de teléfono - fax para la organización donde se asigna esta solicitud o este procedimiento es el 571-273-8300.

La información referida al estado de una solicitud puede obtenerse del sistema de Recuperación de Información de Solicitudes de Patentes (del inglés, Patent Application Information Retrieval (PAIR)). La información sobre el estado para solicitudes publicadas puede obtenerse indistintamente del PAIR privado como del PAIR público. La información sobre el estado de solicitudes no publicadas se encuentra disponible solamente a través del PAI Privado. Para mayor información sobre el sistema PAIR, remítase a <http://pair-direct.uspto.gov>. En el caso de surgir preguntas sobre el acceso al sistema PAIR Privado, comuníquese con el Centro de Comercio Electrónico (EBC) al 866-217-9197 (gratuito). Si necesita asistencia de un

Unidad del arte: 2433

Representante de Atención al Cliente de la USPTO o acceder al sistema de información automática, llame al 800-786-9199 (EN EE. UU. o CANADÁ) o al 571 -272-1000.

/William J. Goodchild/

Examinador Primario, Unidad del arte 2433

EN LA OFICINA DE PATENTES Y MARCAS DE LOS ESTADOS UNIDOS

En la Re-Solicitud de Patente de:	)	Exp. del Abogado	038918-0444639
Marcus ANDRADE		No.:	
Nº de Serie: 15/083.241	)	Nº de confirmación:	5060
Fecha de presentación: 28 de marzo de 2016	)	Examinador:	William J. Goodchild
	)	Unidad del arte:	2433

Para: SISTEMA Y MÉTODO PARA PROPORCIONAR VERIFICACIÓN DE IDENTIDAD
PERSONAL MULTIFACTORIAL BASADA EN LA CADENA DE BLOQUEO

RESPUESTA A LA VISTA NO FINAL ENVIADA EL 18 DE OCTUBRE DE 2017

ENMIENDA DE DIRECCIÓN POSTAL

Comisionado de Patentes
P.O. Box 1450 Alexandria,
VA. 22313-1450

Estimado Sr.:

En respuesta a la Vista No Final enviada el **18 de octubre de 2017** (de aquí en adelante “Vista”), sírvase enmendar la solicitud identificada anteriormente de la siguiente manera:

Las **Enmiendas a las reivindicaciones** comienzan en la
página **2** de este documento. Los **Comentarios** comienzan
en la página **10** de este documento.

No se considera que se requieran extensiones de tiempo o aranceles para la incorporación neta de las reivindicaciones más allá de las que se pueden proveer de otro modo en los documentos que acompañan este documento. Sin embargo, si son necesarias extensiones de tiempo adicionales para evitar el abandono de esta solicitud, entonces dichas extensiones de tiempo se solicitan mediante este documento de acuerdo con 37 C.F.R. § 1.136(a), y cualquier arancel requerido (incluso los aranceles por la incorporación neta de reivindicaciones) se autorizan mediante este documento para cargar a la Cuenta de Depósito Nº 033975 (**Ref. Nº 038918-0444639**).

Esta lista de reivindicaciones reemplazará a las versiones y listas anteriores en la Solicitud.

LISTING OF CLAIMS:

1-20. (Canceladas)

21. (Nueva) Un sistema para proporcionar verificación de identidad personal multifactorial basada en cadena de bloques, caracterizado porque el sistema comprende:

uno o más medios de almacenamiento legibles por computadora para almacenar una cadena de bloques; un sistema informático instalado en un servidor que comprende uno o más procesadores programados para ejecutar instrucciones del programa informático que, cuando se ejecuta, hace que el sistema informático instalado en el servidor:

asignar una dirección de verificación asociada con la cadena de bloques a un individuo, donde el individuo tiene una identidad personal previamente verificada;

almacenar, en uno o más medios de almacenamiento legibles por computadora, un identificador del individuo y el resumen biométrico del individuo en asociación con la dirección de verificación asociada con la cadena de bloques,

donde el resumen biométrico es un resumen de los datos biométricos del individuo, y

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

obtener, de un dispositivo del cliente, el identificador y los datos biométricos en conexión con una solicitud para verificar la identidad del individuo, donde la solicitud indica la dirección de verificación asociada con la cadena de bloques;

obtener el identificador almacenado y el resumen biométrico almacenado con el uso de la dirección de verificación indicada en la solicitud; y

firmar la verificación de la identidad del individuo en respuesta a una determinación de que el identificador de la solicitud y los datos biométricos de la solicitud coinciden con el identificador almacenado y el resumen biométrico almacenado.

22. **(Nueva)** El sistema de acuerdo con la reivindicación 21, caracterizado porque se hace que el sistema informático instalado en el servidor: firme, con el uso de la llave privada de cuya dirección de verificación derivó, la verificación de la identidad del individuo en respuesta a la determinación de que el identificador de la solicitud y los datos biométricos de la solicitud coinciden con el identificador almacenado y el resumen biométrico almacenado.
23. **(Nueva)** El sistema de acuerdo con la reivindicación 22, caracterizado porque se hace que el sistema informático instalado en el servidor: almacene, en uno o más medios de almacenamiento legibles por computadora, la llave privada en asociación con la dirección de verificación asociada con la cadena de bloques; obtener, del dispositivo del cliente, la llave privada en conexión con la solicitud para verificar la identidad del individuo; obtener la llave privada almacenada con el uso de la dirección de verificación indicada en la solicitud; y firmar, con el uso de la llave privada, la verificación de la identidad del individuo en respuesta a una determinación de que el identificador de la solicitud, los datos biométricos de la solicitud, y la llave privada de la solicitud coinciden con el identificador almacenado, el resumen biométrico almacenado y la llave privada almacenada.
24. **(Nueva)** El sistema de acuerdo con la reivindicación 23, caracterizada porque la llave privada también se almacena en el dispositivo del cliente, y donde el dispositivo del cliente es un dispositivo de usuario del individuo.
25. **(Nueva)** El sistema de acuerdo con la reivindicación 21, caracterizado porque se hace que el sistema informático instalado en el servidor: asigne otra dirección de verificación asociada con la cadena de bloques del individuo; almacene, en uno o más medios de almacenamiento legibles por computadora, otro resumen biométrico del individuo en asociación con la otra dirección de verificación asociada con la cadena de bloques, donde el otro resumen biométrico es un resumen de otros datos biométricos del individuo; obtener, del dispositivo del cliente, los otros datos biométricos en conexión con la solicitud para verificar la identidad del individuo, donde la solicitud indica, además, la otra dirección de verificación asociada con la cadena de bloques; obtener el otro resumen biométrico almacenado con el uso de la otra dirección de verificación indicada en la solicitud; y

firmar la verificación de la identidad del individuo en respuesta a una determinación de que el identificador de la solicitud, los datos biométricos de la solicitud, y los otros datos biométricos de la solicitud coinciden con el identificador almacenado, el resumen biométrico almacenado y el otro resumen biométrico almacenado.

26. **(Nueva)** El sistema de acuerdo con la reivindicación **25**, caracterizado porque se hace que el sistema informático instalado en el servidor : obtenga, a través de una interfaz de usuario, un comando iniciado por el usuario para agregar la otra dirección de verificación como una dirección de la cadena de bloques para el individuo; y
asignar la otra dirección de verificación asociada con la cadena de bloques al individuo en base al comando iniciado por el usuario.

27. **(Nueva)** El sistema de acuerdo con la reivindicación **25**, caracterizado porque se hace que el sistema informático instalado en el servidor : obtenga, a través de una interfaz de usuario, un comando iniciado por el usuario para quitar la otra dirección de verificación como una dirección de la cadena de bloques para el individuo; y
desasociar la otra dirección de verificación asociada con la cadena de bloques del individuo en base al comando iniciado por el usuario.

28. **(Nueva)** El sistema de acuerdo con la reivindicación **21**, caracterizado porque se hace que el sistema informático instalado en el servidor: proporcione un primer usuario, diferente del individuo, acceda a los datos almacenados en el uno o más
medios de almacenamiento legibles por computadora en asociación con la dirección de verificación asociada con la cadena de bloques, donde al primer usuario se le brinda acceso a los datos almacenados en base a la verificación de que el primer usuario tiene una primera llave privada, donde la primera llave privada es diferente de la llave privada de la cual derivó la dirección de verificación; y

denegar a un segundo usuario, distinto del individuo, acceso a los datos almacenados en base a la verificación de que el segundo usuario tiene una segunda llave privada.

29. **(Nueva)** El sistema de acuerdo con la reivindicación **21**, caracterizado porque los datos biométricos comprenden una imagen, una grabación o un patrón.

30. **(Nueva)** El sistema de acuerdo con la reivindicación 21, caracterizado porque los datos biométricos se relacionan con una huella digital, las venas de la palma, el reconocimiento facial, el ADN, la impresión palmar, la geometría de la mano, el reconocimiento del iris, la retina, el olor, el andar o la voz.

31. **(Nueva)** Un método para proporcionar la verificación de la identidad personal multifactorial en base a la cadena de bloques, donde el método está implementado por medio de un sistema informático instalado en el servidor que comprende uno o más procesadores que ejecutan instrucciones de programas informáticos que, cuando se ejecutan, realizan el método, el método está caracterizado porque comprende:

- almacenar, mediante el sistema informático instalado en el servidor, una cadena de bloques en uno o más medios de almacenamiento legibles por computadora del sistema informático instalado en el servidor;

- asignar, mediante el sistema informático instalado en el servidor, una dirección de verificación asociada con la cadena de bloques a un individuo, donde el individuo tiene una identidad personal previamente verificada;

- almacenar, mediante el sistema informático instalado en el servidor, en uno o más medios de almacenamiento legibles por computadora, un identificador del individuo y el resumen biométrico del individuo en asociación con la dirección de verificación asociada con la cadena de bloques,

 - donde el resumen biométrico es un resumen de los datos biométricos del individuo, y donde cada uno del identificador, el resumen biométrico y la dirección de verificación son diferentes entre sí y son diferentes de las llaves privadas y públicas de las cuales derivó la dirección de verificación;

- obtener, mediante el sistema informático instalado en el servidor, de un dispositivo del cliente, el identificador y los datos biométricos en conexión con una solicitud para verificar la identidad del individuo, donde la solicitud indica la dirección de verificación asociada con la cadena de bloques;

- obtener, mediante el sistema informático instalado en el servidor, el identificador almacenado y el resumen biométrico almacenado con el uso de la dirección de verificación indicada en la solicitud; y

- asignar, mediante el sistema informático instalado en el servidor, la verificación de la identidad del individuo en respuesta a una determinación de que el identificador de la solicitud y los datos biométricos de la solicitud coinciden con el identificador almacenado y el resumen biométrico almacenado.

32. **(Nueva)** El método de acuerdo con la reivindicación 31, caracterizado porque comprende:

- firmar, mediante el sistema informático instalado en el servidor, con el uso de la llave privada de la cual derivó la dirección de verificación, la verificación de la identidad del individuo en respuesta a la determinación de que el identificador de la solicitud y los datos biométricos de la solicitud coinciden con el identificador almacenado y el resumen biométrico almacenado.

33. **(Nueva)** El método de acuerdo con la reivindicación **32**, caracterizado porque comprende:
almacenar, mediante el sistema informático instalado en el servidor, en uno o más medios de almacenamiento legibles por computadora, la llave privada en asociación con la dirección de verificación asociada con la cadena de bloques,

obtener, mediante el sistema informático instalado en el servidor, del dispositivo del cliente, la llave privada en conexión con la solicitud para verificar la identidad del individuo; obtener la llave privada almacenada con el uso de la dirección de verificación indicada en la solicitud; y

firmar, mediante el sistema informático instalado en el servidor, con el uso de la llave privada, la verificación de la identidad del individuo en respuesta a una determinación de que el identificador de la solicitud, los datos biométricos de la solicitud, y la llave privada de la solicitud coinciden con el identificador almacenado, el resumen biométrico almacenado y la llave privada almacenada.

34. **(Nueva)** El método de acuerdo con la reivindicación 31, caracterizado porque comprende:
asignar, mediante el sistema informático instalado en el servidor, otra dirección de verificación asociada con la cadena de bloques al individuo;

almacenar, mediante el sistema informático instalado en el servidor, en uno o más medios de almacenamiento legibles por computadora, otro resumen biométrico del individuo en asociación con la otra dirección de verificación asociada con la cadena de bloques, donde el otro resumen biométrico es un resumen de otros datos biométricos del individuo;

obtener, mediante el sistema informático instalado en el servidor, del dispositivo del cliente, los otros datos biométricos en conexión con la solicitud para verificar la identidad del individuo, donde la solicitud indica, además, la otra dirección de verificación asociada con la cadena de bloques;

obtener, mediante el sistema informático instalado en el servidor, el otro resumen biométrico almacenado con el uso de la otra dirección de verificación indicada en la solicitud; y

firmar, mediante el sistema informático instalado en el servidor, la verificación de la identidad del individuo en respuesta a una determinación de que el identificador de la solicitud, los datos biométricos de la solicitud, y los otros datos biométricos de la solicitud coinciden con el identificador almacenado, el resumen biométrico almacenado y el otro resumen biométrico almacenado.

35. **(Nueva)** El método de acuerdo con la reivindicación **34**, caracterizado porque comprende: obtener, mediante el sistema informático instalado en el servidor, a través de una interfaz de usuario, un comando iniciado por el usuario para agregar la otra dirección de verificación como dirección de la cadena de bloques para el individuo; y
asignar, mediante el sistema informático instalado en el servidor, la otra dirección de verificación asociada con la cadena de bloques al individuo en base al comando iniciado por el usuario.
36. **(Nueva)** El método de acuerdo con la reivindicación **34**, caracterizado porque comprende: obtener, mediante el sistema informático instalado en el servidor, a través de una interfaz de usuario, un comando iniciado por el usuario para quitar la otra dirección de verificación como dirección de la cadena de bloques para el individuo; y
desasociar, mediante el sistema informático instalado en el servidor, la otra dirección de verificación asociada con la cadena de bloques del individuo en base al comando iniciado por el usuario.
37. **(Nueva)** El método de acuerdo con la reivindicación **31**, caracterizado porque comprende: proporcionar, mediante el sistema informático instalado en el servidor, a un primer usuario, diferente del individuo, acceso a los datos almacenados en el uno o más medios de almacenamiento legibles por computadora en asociación con la dirección de verificación asociada con la cadena de bloques, donde al primer usuario se le brinda acceso a los datos almacenados en base a la verificación de que el primer usuario tiene una primera llave privada, donde la primera llave privada es diferente de la llave privada de la cual derivó la dirección de verificación; y
denegar, mediante el sistema informático instalado en el servidor, a un segundo usuario, distinto del individuo, acceso a los datos almacenados en base a la verificación de que el segundo usuario tiene una segunda llave privada.
38. **(Nueva)** El método de acuerdo con la reivindicación **31**, caracterizado porque los datos biométricos comprenden una imagen, una grabación o un patrón.
39. **(Nueva)** El método de acuerdo con la reivindicación **31**, caracterizado porque los datos biométricos se relacionan con una huella digital, las venas de la palma, el reconocimiento facial, el ADN, la impresión palmar, la geometría de la mano, el reconocimiento del iris, la retina, el olor, el andar o la voz.

40. **(Nueva)** Un sistema para proporcionar verificación de identidad personal multifactorial basada en cadena de bloques, caracterizado porque el sistema comprende:

uno o más medios de almacenamiento legibles por computadora para almacenar una cadena de bloques; un sistema informático instalado en un servidor que comprende uno o más procesadores programados para ejecutar instrucciones del programa informático que, cuando se ejecuta, hace que el sistema informático instalado en el servidor:

asignar múltiples direcciones de verificación de la cadena de bloques al individuo, donde el individuo tiene una identidad personal verificada previamente, donde 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;

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

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

donde cada uno del identificador, el primer resumen biométrico, el segundo resumen biométrico, la primera dirección de verificación y la segunda dirección de verificación son diferentes una de otra, diferentes de las primeras llaves privada y pública de las cuales derivó la primera dirección de verificación, y diferentes de las segundas llaves privada y pública de las cuales derivó la segunda dirección de verificación; obtener, de un dispositivo del cliente, el identificador, los primeros datos biométricos, y los segundos datos biométricos en conexión con una solicitud para verificar la identidad del individuo, donde la solicitud indica la primera dirección de verificación asociada con la cadena de bloques y la segunda dirección de verificación asociada con la cadena de bloques;

obtener (i) el identificador almacenado y el primer resumen biométrico almacenado, con el uso de la primera dirección de verificación indicada en la solicitud y (ii) el segundo resumen biométrico almacenado con el uso de la segunda dirección de verificación indicada en la solicitud; y

firmar, con el uso de la llave privada de la cual derivó la primera dirección de verificación,

la verificación de la identidad del individuo en respuesta a una determinación de que el identificador de la solicitud, los primeros datos biométricos de la solicitud, y los segundos datos biométricos de la solicitud coinciden con el identificador almacenado, el resumen biométrico almacenado y el segundo resumen biométrico almacenado;

proporcionar a un primer usuario, diferente del individuo, acceso a los datos almacenados en el uno o más medios de almacenamiento legibles por computadora en asociación con la primera dirección de verificación asociada con la cadena de bloques, donde al primer usuario se le brinda acceso a los datos almacenados en base a la verificación de que el primer usuario tiene una primera llave privada, donde la primera llave privada es diferente de la llave privada de la cual derivó la primera dirección de verificación y diferente de la llave privada de la cual derivó la segunda dirección de verificación; y

denegar a un segundo usuario, distinto del individuo, acceso a los datos almacenados en base a la verificación de que el segundo usuario tiene una segunda llave privada.

COMENTARIOS

Mediante esta respuesta, las reivindicaciones 1-20 se han cancelado sin perjuicio ni descargo de responsabilidad, y las reivindicaciones 21-40 se han agregado nuevas. Por lo tanto, las reivindicaciones 21-40 ahora están pendientes. Se proporciona soporte para las presentes enmiendas en toda la Memoria Descriptiva tal como se presentó. De este modo, no se ha agregado ningún nuevo tema. En vista de las enmiendas que anteceden y de los siguientes comentarios, se solicita respetuosamente la concesión de todas las reivindicaciones pendientes en la solicitud.

35 U.S.C. §§ 102/103 RECHAZOS

El Solicitante está de acuerdo con la corrección del rechazo del arte previo. No obstante, exclusivamente para avanzar con el seguimiento de este caso, el Solicitante ha modificado el pliego de reivindicaciones pendientes. Las referencias en las que se basa la Vista no enseñan ni sugieren el pliego de reivindicaciones pendientes (como al menos el modificado actualmente). Como ejemplo, la Publicación de la Solicitud de Patente de EE. UU. N° 2015/0324789 concedida a Dvorak *et al*, (“Dvorak”) no enseña las siguientes características de la reivindicación 1:

[se hace que] un sistema informático instalado en el servidor:

asigne una dirección de verificación asociada con la cadena de bloques a un individuo...;

almacenar, en el ... medio de almacenamiento legible por computadora [del sistema informático instalado en el servidor], un identificador del individuo y un resumen biométrico del individuo en asociación con la dirección de verificación asociada con la cadena de bloques,

donde el resumen biométrico es un resumen de los datos biométricos del individuo, y

donde cada uno del identificador, el resumen biométrico y la dirección de verificación son diferentes entre sí y diferentes de las llaves privada y pública de la cual derivó la dirección de verificación;

obtener, de un dispositivo del cliente, el identificador y los datos biométricos en conexión con una solicitud para verificar la identidad del individuo, donde la solicitud indica la dirección de verificación asociada con la cadena de bloques; ... y

firmar la verificación de la identidad del individuo en respuesta a una determinación de que el identificador de la solicitud y los datos biométricos de la solicitud coincidan con el identificador almacenado y el resumen biométrico almacenado.

Las reivindicaciones independientes 31 y 40 incluyen recitados similares,

Ninguna otra referencia considerada supera las deficiencias anteriores de Dvorak. La Vista no alega de otro modo.

Fecha de presentación: 28 de marzo de 2016

Al menos por los siguientes motivos, el Solicitante solicita respetuosamente el retiro de los rechazos del arte previo. Las reivindicaciones dependientes también son susceptibles de concesión porque finalmente dependen de una reivindicación independiente, además de por las características adicionales que recitan.

CONCLUSIÓN

Luego de haber abordado cada uno de los siguientes rechazos, se presenta respetuosamente que se ha realizado una respuesta total y completa de la Vista pendiente y, como tal, la solicitud se encuentra en condición de concesión. Se solicita respetuosamente notificación a tal efecto.

Si el Examinador considera, por cualquier motivo, que la comunicación personal acelerará el seguimiento de esta solicitud, se invita al Examinador a llamar por teléfono al número provisto.

Fecha: 19 de diciembre de 2017

N° de cliente: 00909

Atentamente,

PILLSBURY WINTHROP SHAW PITTMAN LLP

Por: /Ngai B. Zhang/

Ngai B. Zhang

N° de registro 65.473

P.O. Box 10500

McLean, Virginia 22102

Número directo: 703.770.7532

Principal: 703.770.7900

Fax: 703.770.7901



OFICINA DE PATENTES Y MARCAS DE ESTADOS UNIDOS

DEPARTAMENTO DE COMERCIO DE ESTADOS UNIDOS

Oficina de patentes y marcas de estados unidos

Domicilio: COMISIONADO DE PATENTES

P.O. Box 1450

Alexandria, Virginia 22313-1450 www.uspto.gov

Nº DE SOLICITUD	FECHA DE PRESENTACIÓN	PRIMER INVENTOR NOMBRADO	Nº DE EXP. DEL ABOGADO	Nº DE CONFIRMACIÓN
15/083.241	28/03/2016	Marcus Andrade	038918-0444639	5060

909 7590 18/10/2017
Pillsbury Winthrop Shaw Pittman, LLP
PO Box 10500
McLean, VA 22102

EXAMINADOR GOODCHILD, WILLIAM J

UNIDAD DEL ARTE 2433	NÚMERO DE DOCUMENTO
-------------------------	---------------------

FECHA DE Notificación 18/10/2017	MODO DE ENTREGA ELECTRÓNICA
-------------------------------------	--------------------------------

Sírvase encontrar abajo y/o adjunta una comunicación de la Oficina referida a esta solicitud o a este procedimiento.

El período de tiempo para responder, si lo hay, se establece en la comunicación adjunta.

La notificación de la comunicación de la Oficina se envió electrónicamente en la "Fecha de Notificación" indicada más arriba a la(s) siguiente(s) dirección(es) de e-mail:

docket_ip @pillsburylaw.com

Resumen de la Vista

Nº DE SOLICITUD	Solicitante(s)	
15/083.241	ANDRADE, MARCUS	
Examinador	Unidad del	Estado de AIA (Primer inventor en archivo) Sí
WILLIAM GOODCHILD	arte	

- La FECHA DE ENVÍO de esta comunicación aparece en la carátula con la dirección de correspondencia —

Período de respuesta

SE FIJA UN PERÍODO ABREVIADO POR LEY QUE VENCE EN 3 MESES PARA RESPONDER DESDE LA FECHA DE ESTA COMUNICACIÓN.

- Pueden estar disponibles extensiones de tiempo según las disposiciones de 37 CFR 1.136(a). En ningún caso, sin embargo, se puede presentar oportunamente una respuesta después de SEIS (6) MESES desde la fecha de esta comunicación.
- Si NO se especifica anteriormente período para la respuesta, aplicará el período máximo por ley y vencerá SEIS (6) MESES después de la fecha de esta comunicación.
- La falta de respuesta dentro del período establecido o extendido, por ley, hará que la solicitud quede ABANDONADA (35 U.S.C. § 133). Cualquier respuesta recibida por la Oficina después de los tres meses posteriores a la fecha de envío de esta comunicación, incluso si se presenta oportunamente, puede reducir el ajuste del plazo de patente ganado. Véase 37 CFR 1.704(b).

Estado

- 1) ☒ En respuesta a la(s) comunicación(es) presentadas el 28/03/2016.
☐ Una declaración(es)/declaración(es) jurada(s) según **37 CFR 1.130(b)** se presentó/se presentaron el _____
- 2a) ☐ Esta vista es **FINAL**. 2b) ☒ Esta vista no es final.
- 3) ☐ El solicitante realizó una elección en respuesta a un requerimiento de restricción establecido durante la entrevista el _____; el requerimiento de restricción y la elección se han incorporado en esta vista.
- 4) ☐ Dado que esta solicitud está en condición de concederse, excepto por cuestiones formales, el seguimiento de acuerdo con el mérito se cierra de acuerdo con la práctica según *Ex parte Quayle*, 1935 C.D. 11,453 O.G. 213.

Disposición de reivindicaciones*

- 5) ☒ La(s) Reivindicación(s) 1-20 está/están pendientes en la solicitud.
5a) De la(s) reivindicación(es) anterior(es) _____ se retira/n de consideración.
- 6) ☐ La(s) reivindicación(es) _____ se concede/n.
- 7) ☒ La(s) reivindicación(es) 1-20 se rechaza/n.
- 8) ☐ La(s) reivindicación(es) _____ se objeta/n.
- 9) ☐ La(s) reivindicación(es) _____ se someten a requerimiento de restricción y/o elección.

* Si se hubiera determinado que cualquiera de las reivindicaciones es apta para concederse, Ud. puede ser elegible para el beneficio del programa de **Seguimiento Acelerado de Patente** en una oficina participativa de la propiedad intelectual para la solicitud correspondiente. Para mayor información, remítase a <http://www.uspto.gov/patents/init events/pph/index.jsp> o envíe una consulta a PPHfeedback@uspto.gov.

Documentos de la Solicitud

- 10) ☐ La memoria descriptiva está objetada por el Examinador.
- 11) ☐ El(los) dibujo(s) presentado(s) el _____ es/son: a) ☐ aceptado(s) o b) ☐ objetado(s) por el Examinador.
El solicitante no puede solicitar que ninguna objeción al(a los) dibujo(s) queden pendientes. Véase 37 CFR 1.85(a). Se requiere el reemplazo de la(s) hoja(s) de dibujos que incluyan la corrección requerida en el(los) dibujo(s). Véase 37 CFR 1.121 (d).

Prioridad según 35 U.S.C. § 119

- 12) ☐ Se declara conocimiento de una reivindicación de prioridad extranjera según lo dispuesto en 35 U.S.C. § 119(a)-(d) o (f).

Copias certificadas:

- a) ☐ Todas b) ☐ Algunas** c) ☐ Ninguna de las:

1. ☐ Copias certificadas de los documentos de prioridad se han recibido.
2. ☐ Copias certificadas de los documentos de prioridad se han recibido en el Nº de Solicitud _____.
3. ☐ Copias certificadas de los documentos de prioridad se han recibido en esta solicitud en Etapa Nacional de la Oficina Internacional (Regla PCT 17.2(a)).

** Véase la Vista detallada adjunta para conocer la lista de las copias certificadas no recibidas.

Anexo(s)

- 1) ☒ Notificación de Referencias Citadas (PTO-892)
- 2) ☒ Declaración(es) de Divulgación de Información (PTO/SB/O8a y/o PTO/SB/O8b)
Nº de Documento(s) /Fecha de envío 19/09/2016
- 3) ☐ Resumen de la entrevista (PTO-413)
Nº de Documento(s) /Fecha de envío _____
- 4) ☐ Otro: _____

ACCIÓN DETALLADA

Notificación de Estado Pre-AIA o AIA

1. La presente solicitud, presentada del 16 de marzo de 2013 en adelante, se somete a examen según las disposiciones del primer inventor en presentar de AIA.

Rechazos de reivindicaciones - 35 USC §102

1. Lo que sigue es una transcripción de los párrafos apropiados de 35 U.S.C. 102 que forman la base de los rechazos según esta sección realizados en esta Vista:

Una persona estará habilitada a una patente a menos que -

(a)(1) la invención reivindicada estuviera patentada, descrita en una publicación impresa, en uso público, en venta o de otro modo disponible al público antes de la fecha de presentación efectiva de la invención reivindicada.

(a)(2) la invención reivindicada estuviera descrita en una patente concedida según la sección 151, o en una solicitud para patente publicada o considerada publicada de acuerdo con la sección 122(b), en la cual la patente o la solicitud, según sea el caso, nombre a otro inventor y se presentara efectivamente antes de la fecha de presentación de la invención reivindicada.

2. La(s) reivindicación(es) 1-3, 5-15 y 17-20 están rechazadas de acuerdo con 35 U.S.C. 102(a)(1) y (a)(2) como lo anticipa Dvorak et al., (Nº de Publicación de EE. UU. 2015/0324789), de aquí en adelante "Dvorak".

Respecto de las reivindicaciones **1, 14 y 18**, Dvorak divulga proporcionar verificación de identidad personal multifactorial en base a cadena de bloques [Dvorak, Resumen y párrafo 60]:
uno o más procesadores de hardware configurados por instrucciones legibles por computadora [Dvorak, párrafos 58 y 59] para:

establecer direcciones de verificación en una cadena de bloques mediante: la asociación de los identificadores con los individuos que tienen identidades personales previamente verificadas, un primer identificador asociado a un primer individuo, donde un primer individuo tiene una identidad personal previamente verificada [Dvorak, párrafos 80, 82-84, 111 y 112];

asignar direcciones de verificación en una cadena de bloques a los individuos, donde una dirección de verificación dada que incluye una llave pública y una llave privada, donde la primera dirección de verificación está asignada al primer individuo, donde la primera dirección de verificación incluye una primera llave pública y una primera llave privada [Dvorak, párrafos 59, 112 and 113]; y

registrar identificadores y datos biométricos asociados con los individuos en las correspondientes direcciones de verificación, donde el primer identificador y los primeros datos biométricos asociados con el primer individuo se registran en la primera dirección de verificación [Dvorak, párrafos 94 and 98]; y

realizar la verificación de identidad personal multifactorial en base a la cadena de bloques con el uso de las direcciones de verificación [Dvorak, párrafo 59] mediante: recepción de uno o más identificadores en conexión con una o más solicitudes para verificar la identidad de uno o más individuos, donde el primer identificador se recibe en conexión con una solicitud de verificar una identidad del primer individuo [Dvorak, párrafos 58, 62-65, 72 y 94];

extraer los datos biométricos asociados con uno o más individuos de las correspondientes direcciones de verificación, donde los primeros datos biométricos asociados con el primer individuo se extraen de la primera dirección de [Dvorak, párrafos 58 and 67]; y

15/083.241

verificar la identidad del uno o más individuos tras recibir los datos biométricos coincidentes y donde las llaves privadas, la identidad personal del primer individuo se verifican tras la recepción de (1) los datos biométricos coincidentes con los primeros datos biométricos y (2) una llave privada coincidente con la primera llave privada [Dvorak, párrafos 57, 67 y 94],

Respecto de la reivindicación 2, Dvorak divulga, además, donde la primera llave privada se almacena dentro de una plataforma informática asociada con el primer individuo [Dvorak, párrafo 67].

Respecto de las reivindicaciones 3 y 15, Dvorak divulga, además, donde múltiples direcciones de verificación se asignan a individuos separados de modo tal que, además de la primera dirección de verificación, una segunda dirección de verificación se asigna al primer individuo [Dvorak, párrafo 59].

Respecto de las reivindicaciones 5 and 17, Dvorak divulga, además, donde se registran diferentes datos biométricos en múltiples direcciones de verificación asignadas a un individuo dado de modo tal que, además del primer identificador y los primeros datos biométricos asociados con el primer individuo se registran en la primera dirección de verificación, el primer identificador y los segundos datos biométricos asociados con el primer individuo se registran en la segunda dirección de verificación [Dvorak, párrafos 59, 84 y 98].

Respecto de la reivindicación 8, Dvorak divulga, además, donde la identidad personal del primer individuo se verifica tras la recepción de (1) los datos biométricos coincidentes con los primeros datos biométricos o los segundos datos biométricos y (2) una llave privada coincidente con la primera llave privada [Dvorak, párrafos 90, 51,94 y 59].

Respecto de la reivindicación 7, Dvorak divulga, además, donde los datos biométricos incluyen uno o más de una imagen, una grabación o un patrón [Dvorak, párrafo 59].

Respecto de la reivindicación 8, Dvorak divulga, además, donde los datos biométricos se relacionan con uno o más de una huella digital, las venas palmares, el reconocimiento facial, ADN, impresión palmar, geometría de la mano, reconocimiento del iris, retina, olor o perfume, ritmo de tipeo, andar o voz [Dvorak, párrafos 90 y 51],

Respecto de la reivindicación 9, Dvorak divulga, además, donde los primeros datos biométricos se reciben a través de una plataforma informática asociada con el primer individuo [Dvorak, párrafo 67].

Respecto de la reivindicación 10, Dvorak divulga, además, donde el uno o más procesadores de hardware está/n configurado/s mediante instrucciones legibles por computadora para, en respuesta a recibir la solicitud de verificar la identidad del primer individuo, impulsa al primer individuo para dar los datos biométricos coincidentes con los primeros datos biométricos

y una llave privada coincidente con la primera llave privada, donde la entrada se transporta a través de una plataforma informática asociada con el primer individuo [Dvorak, párrafos 90, 51 y 67],

Respecto de la reivindicación 11, Dvorak divulga, además, donde el uno o más procesadores de hardware están configurados, además, mediante instrucciones legibles por computadora en respuesta a recibir la solicitud de verificar la identidad del primer individuo, entrar a una plataforma informática asociada con el primer individuo para proporcionar automáticamente los datos biométricos coincidentes con los primeros datos biométricos y una llave privada coincidente con la primera llave privada [Dvorak, párrafos 90, 51, 94 y 87],

Respecto de las reivindicaciones 12 y 20, Dvorak divulga, además, donde los datos biométricos coincidentes con los primeros datos biométricos y la llave privada coincidente con la primera llave privada se usan para firmar la verificación de la identidad personal del primer individuo [Dvorak, párrafo 51].

Respecto de la reivindicación 13, Dvorak divulga, además, donde al menos un nodo exclusivo realiza la firma de la verificación de la identidad personal del primer individuo [Dvorak, párrafo 52],

Respecto de la reivindicación 19, Dvorak divulga, además,

15/083.241

en respuesta a recibir la solicitud de verificar la identidad del primer individuo:

instar al primer individuo para obtener los datos biométricos coincidentes con los primeros datos biométricos y una llave privada coincidente con la primera llave privada, donde la entrada se transporta a través de una plataforma informática asociada con el primer individuo [Dvorak, párrafos 90, 51 y 67]; o

instar a la plataforma informática asociada con el primer individuo a proporcionar automáticamente los datos biométricos coincidentes con los primeros datos biométricos y una llave privada coincidente con la primera llave privada [Dvorak, párrafos 90, 51, 94 y 87].

Rechazos de reivindicaciones - 35 USC §103

3. Lo que sigue es una cita de 35 U.S.C. 103 que forma la base de todas los rechazos por obviedad establecidos en esta Vista:

No puede obtenerse una patente para una invención reivindicada, no obstante que la invención reivindicada no sea divulgada de manera idéntica como se establece en el artículo 102, si las diferencias entre la invención reivindicada y el arte previo son tales que la invención reivindicada como un todo hubiera sido obvia antes de la fecha efectiva de presentación de la invención reivindicada para una persona con experiencia normal en el arte al cual pertenece la invención reivindicada. No se negará la patentabilidad por el modo en que se realizó la invención.

4. Las reivindicaciones 4 y 16 se rechazan según 35 U.S.C. 103 por no ser patentables por sobre Dvorak según lo aplicado a las reivindicaciones 1 y 14 anteriores, y además, en vista de Pennanen, (Publicación de EE. UU. N° 2015/0356555).

Respecto de las reivindicaciones 4 y 16, Dvorak divulga, además, donde el uno o más procesadores de hardware están configurados, además, mediante instrucciones legibles por computadora para proporcionar una interfaz para presentación a los individuos a través de plataformas informáticas asociadas [Dvorak, párrafo 58].

Dvorak no divulga específicamente

la interfaz que está configurada para permitir que un individuo dado agregue o elimine las direcciones de verificación asignadas al individuo dado en tanto que al menos una dirección de verificación esté asignada al individuo dado.

Sin embargo, Pennanen enseña un sistema para implementar al menos una transacción de en criptomoneda en un punto de venta mediante la utilización de una terminal móvil [Pennanen, Resumen] y divulga agregar o eliminar direcciones de verificación asignadas al individuo dado en tanto que al menos se de una dirección de verificación [Pennanen, párrafo 88 y figura 2].

Hubiera resultado obvio para una persona con experiencia normal en el arte antes de la fecha de presentación efectiva de la invención reivindicada usar las llaves de Pennanen para agregar y eliminar direcciones de un individuo en un sistema de bitcoin de Case para autenticar la criptomoneda.

Conclusión

Nota del Examinador: El Examinador ha citado párrafos / columnas y números de línea particulares en la(s) referencia(s) aplicada(s) a las reivindicaciones que anteceden para la conveniencia del solicitante. Aunque las citas específicas son representativas de las enseñanzas del arte y se aplican a las limitaciones específicas dentro de la reivindicación individual, otros pasajes y figuras pueden aplicar también. Se solicita respetuosamente del solicitante al momento de preparar

las respuestas, que considere totalmente las referencias en su totalidad como enseñanza potencial de toda o parte de la invención, además del contexto de los pasajes citados como lo enseña el arte previo o en los que se basa el examinador. En el caso de que el solicitante enmiende las reivindicaciones de la invención reivindicada, se solicita respetuosamente que el solicitante indique claramente la(s) porción(es) de la memoria descriptiva del solicitante que avalan el léxico de la reivindicación enmendada para aseverar las metas y los límites de la invención reivindicada por el solicitante.

Cualquier consulta referida a esta comunicación o a comunicaciones anteriores del examinador deben dirigirse a WILLIAM GOODCHILD cuyo número de teléfono es (571)270-1589. El examinador puede normalmente encontrarse de Lunes a Viernes / 8:00 - 16:00.

Las entrevistas con el Examinador están disponibles por teléfono, en persona, y por conferencia en video con el uso de una herramienta de colaboración basada en Internet suministrada por la USPTO. Para programar una entrevista, se alienta al solicitante a usar la Solicitud de Entrevista Automática de la USPTO (Automated Interview Request (AIR)) en <http://www.uspto.gov/interviewpractice>.

En el caso de no tener éxito los intentos por comunicarse por el Examinador, se puede comunicar con el supervisor del Examinador, Jeffrey Pwu al (571) 272-6798. El número de teléfono del fax para la organización donde se asigna esta solicitud o procedimiento es el 571-273-8300.

La información referida al estado de una solicitud puede obtenerse del sistema de Recuperación de Información sobre Solicitudes de Patentes (*Patent Application Information Retrieval* (PAIR)). La información sobre el estado para solicitudes publicadas puede obtenerse tanto del PAIR Privado como del PAIR Público. La información del estado para solicitudes no publicadas se encuentra disponible solamente del PAIR Privado. Para obtener información sobre el sistema PAIR, véase <http://pair-direct.uspto.gov>. En el caso de tener preguntas sobre el acceso al sistema PAIR Privado, comuníquese con el Centro Comercial Electrónico (*Electronic Business Center* (EBC)) al 866-217-9197 (sin cargo). Si requiere asistencia de un Representante de Atención al Cliente de la USPTO o acceder al sistema de información automático, llame al 800-786-9199 (EN EE. UU. o CANADÁ) o al 571-272-1000.

/WILLIAM GOODCHILD/

Examinador Primario, Unidad del arte 2433