

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

(Chapter I of the Patent Cooperation Treaty)

(PCT Rule 44bis)

Applicant's or agent's file reference 17-10153-PCT	FOR FURTHER ACTION	See item 4 below
International application No. PCT/US2016/024776	International filing date (<i>day/month/year</i>) 29 March 2016 (29.03.2016)	Priority date (<i>day/month/year</i>) 28 March 2016 (28.03.2016)
International Patent Classification (8th edition unless older edition indicated) See relevant information in Form PCT/ISA/237		
Applicant BLACK GOLD COIN, INC.		

1.	This international preliminary report on patentability (Chapter I) is issued by the International Bureau on behalf of the International Searching Authority under Rule 44 bis.1(a).																								
2.	This REPORT consists of a total of 8 sheets, including this cover sheet.																								
In the attached sheets, any reference to the written opinion of the International Searching Authority should be read as a reference to the international preliminary report on patentability (Chapter I) instead.																									
3.	This report contains indications relating to the following items: <table style="width: 100%;"> <tr> <td style="width: 5%; text-align: center;">☒</td> <td style="width: 25%;">Box No. I</td> <td>Basis of the report</td> </tr> <tr> <td style="text-align: center;">☐</td> <td>Box No. II</td> <td>Priority</td> </tr> <tr> <td style="text-align: center;">☐</td> <td>Box No. III</td> <td>Non-establishment of opinion with regard to novelty, inventive step and industrial applicability</td> </tr> <tr> <td style="text-align: center;">☐</td> <td>Box No. IV</td> <td>Lack of unity of invention</td> </tr> <tr> <td style="text-align: center;">☒</td> <td>Box No. V</td> <td>Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement</td> </tr> <tr> <td style="text-align: center;">☐</td> <td>Box No. VI</td> <td>Certain documents cited</td> </tr> <tr> <td style="text-align: center;">☐</td> <td>Box No. VII</td> <td>Certain defects in the international application</td> </tr> <tr> <td style="text-align: center;">☐</td> <td>Box No. VIII</td> <td>Certain observations on the international application</td> </tr> </table>	☒	Box No. I	Basis of the report	☐	Box No. II	Priority	☐	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability	☐	Box No. IV	Lack of unity of invention	☒	Box No. V	Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement	☐	Box No. VI	Certain documents cited	☐	Box No. VII	Certain defects in the international application	☐	Box No. VIII	Certain observations on the international application
☒	Box No. I	Basis of the report																							
☐	Box No. II	Priority																							
☐	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability																							
☐	Box No. IV	Lack of unity of invention																							
☒	Box No. V	Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement																							
☐	Box No. VI	Certain documents cited																							
☐	Box No. VII	Certain defects in the international application																							
☐	Box No. VIII	Certain observations on the international application																							
4.	The International Bureau will communicate this report to designated Offices in accordance with Rules 44bis.3(c) and 93bis.1 but not, except where the applicant makes an express request under Article 23(2), before the expiration of 30 months from the priority date (Rule 44bis .2).																								

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No. +41 22 338 82 70	Date of issuance of this report 02 October 2018 (02.10.2018) Authorized officer Athina Nickitas-Etienne e-mail: pct.team4@wipo.int
--	--

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To: IAN C. SCHICK, PH.D.
PILLSBURY WINTHROP SHAW PITTMAN LLP
P.O. BOX 10500
MCLEAN, VA 22102

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43bis.1)

Date of mailing
(day/month/year)

16 JUN 2016

Applicant's or agent's file reference
38918-446543

FOR FURTHER ACTION

See paragraph 2 below

International application No.

PCT/US2016/024776

International filing date (day/month/year)

29 March 2016

Priority date (day/month/year)

28 March 2016

International Patent Classification (IPC) or both national classification and IPC

IPC(8) - G06F 17/30; G06Q 20/36; G06Q 20/38 (2016.01)

CPC - G06Q 20/10; G06Q 20/40; G06Q 40/00 (2016.02)

Applicant

BLACK GOLD COIN, INC.

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step and industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. FURTHER ACTION

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1bis(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA/
Mail Stop PCT, Attn: ISA/US
Commissioner for Patents
P.O. Box 1450, Alexandria, VA 22313-1450
Facsimile No. 571-273-8300

Date of completion of this opinion

22 May 2016

Authorized officer

Blaine R. Copenheaver

PCT Helpdesk: 571-272-4300
PCT OSP: 571-272-7774

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.

PCT/US2016/024776

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:
 - ☒ the international application in the language in which it was filed.
 - ☐ a translation of the international application into _____ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).
2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a)).
3. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing:
 - a. ☐ forming part of the international application as filed:
 - ☐ in the form of an Annex C/ST.25 text file.
 - ☐ on paper or in the form of an image file.
 - b. ☐ furnished together with the international application under PCT Rule 13*ter*.1(a) for the purposes of international search only in the form of an Annex C/ST.25 text file.
 - c. ☐ furnished subsequent to the international filing date for the purposes of international search only:
 - ☐ in the form of an Annex C/ST.25 text file (Rule 13*ter*.1(a)).
 - ☐ on paper or in the form of an image file (Rule 13*ter*.1(b) and Administrative Instructions, Section 713).
4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that forming part of the application as filed or does not go beyond the application as filed, as appropriate, were furnished.
5. Additional comments:

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.

PCT/US2016/024776

Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step and industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	4, 16	YES
	Claims	1-3, 5-15, 17-20	NO
Inventive step (IS)	Claims	None	YES
	Claims	1-20	NO
Industrial applicability (IA)	Claims	1-20	YES
	Claims	None	NO

2. Citations and explanations:

Claims 1-3, 5-15, and 17-20 lack novelty under PCT Article 33(2) as being anticipated by Case Wallet Inc (hereinafter Case).

Regarding Claim 1, Case discloses a system for providing block chain-based multifactor personal identity verification (paragraph 94 for having a bitcoin verification system using a virtual wallet with a multifactor identification system with the factions of a private key, a public key, and a fingerprint, with paragraph 59 for using bitcoins on a block chain ledger; paragraph 83 for multifactor authentication, virtual wallet), the system comprising: one or more hardware processors configured by machine-readable instructions to (paragraph 58 for using a server and the internet with one or more processors and a memory to verify the receiver address for the bitcoins): establish verification addresses on a block chain by (paragraph 58 for verifying the receiver address and amount using the block card to validate a bitcoin transaction; also see paragraph 0059 for block chain): associating identifiers with individuals having previously verified personal identities (paragraph 60 for the user providing identifying information to authorize the use of encryption keys and paragraph 98 for having an initial registration with an email, and phone verification for the user or a previously verified personal identity), a first identifier being associated a first individual (paragraph 59 for getting a first identifier or a private encryption key with a block chain ledger and therefore a first bitcoin address, with paragraph 98 for verifying a user or first individual using a first identifier such as a public key and password salt to ensure the password works with the user's account), the first individual having a previously verified personal identity (paragraph 51 for using fingerprints and biometrics to ensure that only verified users are able to carryout a transaction and paragraph 98 for having an initial user setup process that includes verifying the email and phone to link to a secure device); assigning verification addresses on a block chain to the individuals (paragraph 59 for using a block chain ledger that generates a private encryption key and generating addresses on three branches for receiving bitcoins, buying bitcoins and unspent portions of transactions with three randomly generated encryption keys or verification means), a given verification address including a public key and a private key (paragraph 59 for getting a first identifier or a private encryption key with a block chain ledger and therefore a first bitcoin address with paragraph 94 for having a bitcoin verification system using a virtual wallet with a multifactor identification system with the factions of a private key, a public key, and a fingerprint), a first verification address being assigned to the first individual (paragraph 59 for getting a first identifier or a private encryption key with a block chain ledger and therefore a first bitcoin address with a private key for the first individual), the first verification address including a first public key and a first private key (paragraph 59 for getting a first identifier or a private encryption key with a block chain ledger and therefore a first bitcoin address including a private encryption key and three public encryption keys); and recording identifiers and biometric data associated with the individuals at corresponding verification addresses (paragraph 98 for storing or recording identifiers such as an individuals email and salt passwords or means to record identifiers using a web table as well as identifying a secure device with paragraph 94 for using a private key, a public key, and a fingerprint for the user including the user's browser information), the first identifier and first biometric data associated with the first individual being recorded at the first verification address (paragraph 94 for having a first private key identifier and a first fingerprint biometric data associated with an email or user and paragraph 96 for providing cryptocurrency or bitcoin addresses); and perform block chain-based multifactor personal identity verification using the verification addresses by (paragraph 59 for getting a first identifier or a private encryption key with a block chain ledger and therefore a first bitcoin address): receiving one or more identifiers in connection with one or more requests to verify an identity of one or more individuals (paragraph 68-73 for a user receiving bitcoins by clicking a button or having a request for the bitcoin and then swiping the fingerprint scanner for authentication), the first identifier being received in connection with a request to verify an identity of the first individual (paragraph 59 for getting a first identifier or a private encryption key with a block chain ledger and therefore a first bitcoin address and paragraph 94 for using a fingerprint scanner to authenticate the individual); extracting the biometric data associated with the one or more individuals from the corresponding verification addresses (paragraph 67 for getting fingerprint or biometric data and sending the extracted data to a server for authentication and then completing the transaction based on successful authentication), the first biometric data associated with the first individual being extracted from the first verification address (paragraph 67 for the finger print and the stored encryption key being extracted to the server and verified to complete the transfer of bitcoins to their new owner); 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 (1) biometric data matching the first biometric data (paragraph 57 for providing a third authentication fact such as a fingerprint or biometric data means) and (2) a private key matching the first private key (paragraph 94 for having a bitcoin verification system using a virtual wallet with a multifactor identification system with the factions of a private key, a public key and paragraph 59 for having a private encryption key and three public encryption keys).

Regarding Claim 2, Case discloses wherein the first private key is stored within a computing platform associated with the first individual (paragraph 68 for using a block card element 10 associated with the user along with a fingerprint scanner to send a signed transaction to the server using a wireless transceiver element 368).

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.

PCT/US2016/024776

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of:

Regarding Claim 3, Case 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 (paragraph 59 for using a block chain ledger that generates a private encryption key and generating addresses on three branches for receiving bitcoins, buying bitcoins and unspent portions of transactions with three randomly generated encryption keys or verification means along with a private key for the individual to segregate transactions).

Regarding Claim 5, Case 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 (paragraph 94 for having a first private key identifier and a first fingerprint biometric data associated with an email or user and paragraph 96 for providing cryptocurrency or bitcoin addresses), the first identifier and second biometric data associated with the first individual is recorded at the second verification address (paragraph 84 for having multi-signature address generation with multiple keys stored on different servers or second verification addresses on different servers and secure devices to provide additional security).

Regarding Claim 6, Case 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 (paragraph 90 for using a fingerprint scanner to provide authorization information for a secure transaction and paragraph 51 for using multiple biometric readers such as retina, heart rate, for user verification) and (2) a private key matching the first private key (paragraph 94 for having a bitcoin verification system using a virtual wallet with a multifactor identification system with the factions of a private key, a public key and paragraph 59 for having a private encryption key and three public encryption keys).

Regarding Claim 7, Case discloses wherein the biometric data includes one or more of an image, a recording, or a template (paragraph 90 for using a fingerprint scanner to provide authorization information for a secure transaction and paragraph 51 for using multiple biometric readers such as retina, heart rate, for user verification using a scanner or image means for verification).

Regarding Claim 8, Case 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 (paragraph 90 for using a fingerprint scanner to provide authorization information for a secure transaction and paragraph 51 for using multiple biometric readers such as retina, heart rate, for user verification).

Regarding Claim 9, Case discloses wherein the first biometric data is received via a computing platform associated with the first individual (paragraph 68 for using a block card element 10 associated with the user along with a fingerprint scanner to send a signed transaction to the server using a wireless transceiver element 368).

Regarding Claim 10, Case discloses wherein the one or more hardware processors are further configured by machine-readable instructions to (paragraph 58 for using a server and the internet with one or more processors and a memory to verify the receiver address for the bitcoins), responsive to receiving the request to verify the identity of the first individual (paragraph 59 for getting a first identifier or a private encryption key with a block chain ledger and therefore a first bitcoin address and paragraph 94 for using a fingerprint scanner to authenticate the individual), prompt the first individual for biometric data matching the first biometric data and a private key matching the first private key (paragraph 55 for using a block card with input from the user using control buttons for entering the amount of bitcoins to buy and paragraph 57 for the user logging in as the web portal with an encrypted security key as an authentication factor), the prompt being conveyed via a computing platform associated with the first individual (paragraph 57 for using a web portal as a computing platform and a block card associated with the first individual with figure 3 for having a computer platform with means to prompt a user with a menu).

Regarding Claim 11, Case discloses wherein the one or more hardware processors are further configured by machine-readable instructions to (paragraph 58 for using a server and the internet with one or more processors and a memory to verify the receiver address for the bitcoins), responsive to receiving the request to verify the identity of the first individual (paragraph 59 for getting a first identifier or a private encryption key with a block chain ledger and therefore a first bitcoin address and paragraph 94 for using a fingerprint scanner to authenticate the 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 (paragraph 94 for having a bitcoin verification system using a virtual wallet with a multifactor identification system with the factions of a private key, a public key and paragraph 59 for having a private encryption key and three public encryption keys).

Regarding Claim 12, Case 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 (paragraph 21 for having the biometric data or the fingerprint scan match and a first private key to the server where the server matches a second key stored on the server to broadcast a bitcoin transaction with paragraph 51 for having user verification mechanisms so that only authorized users are able to carryout a transaction).

Regarding Claim 13, Case discloses wherein at least one dedicated node performs the signing of the verification of the personal identity of the first individual (paragraph 52 for having a server or node communicating with a transceiver chip for a partially signed bitcoin transaction).

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.

PCT/US2016/024776

Supplemental Box

In case the space in any of the preceding boxes is not sufficient:

Continuation of:

Regarding Claim 14, Case teaches a method for establishing verification addresses on a block chain in order to provide block chain-based multifactor personal identity verification (paragraph 94 for having a bitcoin verification system using a virtual wallet with a multifactor identification system with the factions of a private key, a public key, and a fingerprint, with paragraph 59 for using bitcoins on a block chain ledger; paragraph 83 for multifactor authentication, virtual wallet), the method being performed by one or more hardware processors configured by machine-readable instructions (paragraph 58 for using a server and the internet with one or more processors and a memory to verify the receiver address for the bitcoins), the method comprising: associating identifiers with individuals having previously verified personal identities (paragraph 60 for the user providing identifying information to authorize the use of encryption keys and paragraph 98 for having an initial registration with an email, and phone verification for the user or a previously verified personal identity, with paragraph 59 for getting a first identifier or a private encryption key with a block chain ledger and therefore a first bitcoin address), a first identifier being associated a first individual, the first individual having a previously verified personal identity (paragraph 51 for using fingerprints and biometrics to ensure that only verified users are able to carryout a transaction and paragraph 98 for having an initial user setup process that includes verifying the email and phone to link to a secure device); assigning verification addresses on a block chain to the individuals (paragraph 59 for using a block chain ledger that generates a private encryption key and generating addresses on three branches for receiving bitcoins, buying bitcoins and unspent portions of transactions with three randomly generated encryption keys or verification means), a given verification address including a public key and a private key (paragraph 59 for getting a first identifier or a private encryption key with a block chain ledger and therefore a first bitcoin address with paragraph 94 for having a bitcoin verification system using a virtual wallet with a multifactor identification system with the factions of a private key, a public key, and a fingerprint), a first verification address being assigned to the first individual (paragraph 59 for getting a first identifier or a private encryption key with a block chain ledger and therefore a first bitcoin address with a private key for the first individual), the first verification address including a first public key and a first private key (paragraph 59 for getting a first identifier or a private encryption key with a block chain ledger and therefore a first bitcoin address including a private encryption key and three public encryption keys); and recording identifiers and biometric data associated with the individuals at corresponding verification addresses (paragraph 98 for storing or recording identifiers such as an individuals email and salt passwords or means to record identifiers using a web table as well as identifying a secure device with paragraph 94 for using a private key, a public key, and a fingerprint for the user including the user's browser information), the first identifier and first biometric data associated with the first individual being recorded at the first verification address (paragraph 59 for getting a first identifier or a private encryption key with a block chain ledger and therefore a first bitcoin address with paragraph 94 for having a bitcoin verification system using a virtual wallet with a multifactor identification system with the factions of a private key, a public key, and a fingerprint); wherein the identity of the one or more individuals are verifiable upon receiving matching biometric data and private keys (paragraph 67 for the finger print and the stored encryption key being extracted to the server and verified to complete the transfer of bitcoins to their new owner), the personal identity of the first individual being verifiable upon receipt of (1) biometric data matching the first biometric data (paragraph 57 for providing a third authentication fact such as a fingerprint or biometric data means) and (2) a private key matching the first private key (paragraph 94 for having a bitcoin verification system using a virtual wallet with a multifactor identification system with the factions of a private key, a public key and paragraph 59 for having a private encryption key and three public encryption keys).

Regarding Claim 15, Case teaches assigning multiple verification addresses to separate individuals such that, in addition to the first verification address, a second verification address is assigned to the first individual (paragraph 59 for using a block chain ledger that generates a private encryption key and generating addresses on three branches for receiving bitcoins, buying bitcoins and unspent portions of transactions with three randomly generated encryption keys or verification means along with a private key for the individual to segregate transactions).

Regarding Claim 17, Case teaches recording different biometric data 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 (paragraph 94 for having a first private key identifier and a first fingerprint biometric data associated with an email or user and paragraph 96 for providing cryptocurrency or bitcoin addresses), the first identifier and second biometric data associated with the first individual is recorded at the second verification address (paragraph 84 for having multi-signature address generation with multiple keys stored on different servers or second verification addresses on different servers and secure devices to provide additional security).

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.

PCT/US2016/024776

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of:

Regarding Claim 18, Case teaches method for perform block chain-based multifactor personal identity verification using verification addresses (paragraph 94 for having a bitcoin verification system using a virtual wallet with a multifactor identification system with the factions of a private key, a public key, and a fingerprint, with paragraph 59 for using bitcoins on a block chain ledger; paragraph 83 for multifactor authentication, virtual wallet), the method being performed by one or more hardware processors configured by machine-readable instructions (paragraph 58 for using a server and the internet with one or more processors and a memory to verify the receiver address for the bitcoins), the method comprising: receiving one or more identifiers in connection with one or more requests to verify an identity of one or more individuals (paragraph 60 for the user providing identifying information to authorize the use of encryption keys and paragraph 98 for having an initial registration with an email, and phone verification for the user or a previously verified personal identity, with paragraph 59 for getting a first identifier or a private encryption key with a block chain ledger and therefore a first bitcoin address), a first identifier being received in connection with a request to verify an identity of a first individual (paragraph 51 for using fingerprints and biometrics to ensure that only verified users are able to carryout a transaction and paragraph 98 for having an initial user setup process that includes verifying the email and phone to link to a secure device); extracting biometric data associated with the one or more individuals from corresponding verification addresses on a block chain (paragraph 59 for using a block chain ledger that generates a private encryption key and generating addresses on three branches for receiving bitcoins, buying bitcoins and unspent portions of transactions with three randomly generated encryption keys or verification means), a given verification address including a public key and a private key (paragraph 59 for getting a first identifier or a private encryption key with a block chain ledger and therefore a first bitcoin address with paragraph 94 for having a bitcoin verification system using a virtual wallet with a multifactor identification system with the factions of a private key, a public key, and a fingerprint), first biometric data associated with the first individual being extracted from a first verification address assigned to the first individual (paragraph 59 for getting a first identifier or a private encryption key with a block chain ledger and therefore a first bitcoin address with a private key for the first individual), the first verification address including a first public key and a first private key (paragraph 59 for getting a first identifier or a private encryption key with a block chain ledger and therefore a first bitcoin address including a private encryption key and three public encryption keys); and verifying the identity of the one or more individuals upon receiving matching biometric data and private keys (paragraph 67 for the finger print and the stored encryption key being extracted to the server and verified to complete the transfer of bitcoins to their new owner) the personal identity of the first individual being verified upon receipt of (1) biometric data matching the first biometric data (paragraph 57 for providing a third authentication fact such as a fingerprint or biometric data means) and (2) a private key matching the first private key (paragraph 94 for having a bitcoin verification system using a virtual wallet with a multifactor identification system with the factions of a private key, a public key and paragraph 59 for having a private encryption key and three public encryption keys).

Regarding Claim 19, Case teaches responsive to receiving the request to verify the identity of the first individual (paragraph 58 for using a server and the internet with one or more processors and a memory to verify the receiver address for the bitcoins), responsive to receiving the request to verify the identity of the first individual (paragraph 59 for getting a first identifier or a private encryption key with a block chain ledger and therefore a first bitcoin address and paragraph 94 for using a fingerprint scanner to authenticate the individual); prompting the first individual for biometric data matching the first biometric data and a private key matching the first private key (paragraph 55 for using a block card with input from the user using control buttons for entering the amount of bitcoins to buy and paragraph 57 for the user logging in as the web portal with an encrypted security key as an authentication factor), the prompt being conveyed via a computing platform associated with the first individual (paragraph 57 for using a web portal as a computing platform and a block card associated with the first individual with figure 3 for having a computer platform with means to prompt a user with a menu); 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 (paragraph 94 for having a bitcoin verification system using a virtual wallet with a multifactor identification system with the factions of a private key, a public key and paragraph 59 for having a private encryption key and three public encryption keys).

Regarding Claim 20, Case teaches 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 (paragraph 21 for having the biometric data or the fingerprint scan match and a first private key to the server where the server matches a second key stored on the server to broadcast a bitcoin transaction with paragraph 51 for having user verification mechanisms so that only authorized users are able to carryout a transaction).

Claims 4 and 16 lack an inventive step under PCT Article 33(3) as being obvious over Case Wallet Inc (hereinafter Case) in view of Pennanen.

Regarding Claim 4, Case 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 (paragraph 58 for using a server and the internet with one or more processors and a memory to verify the receiver address for the bitcoins), the interface being configured to allow a given individual for a verification address is assigned to the given individual (paragraph 58 for having a user account server that stores information associated with the user's account by matching the scanned fingerprint against the user's stored fingerprint). Case does not explicitly disclose to add or delete verification addresses assigned to the given individual so long as at least one verification address is given. Pennanen has a system for implementing at least one cryptocurrency transaction at a point-of-sale by using a mobile terminal (abstract) and discloses to add or delete verification addresses assigned to the given individual so long as at least one verification address is given (figure 2 for having a user interface for entering a pay to address element 208 with paragraph 68 for having a user interface for facilitating bitcoin transactions and paragraph 51 for having a means to delete keys once a currency has been authenticated). It would have been obvious to one of ordinary skill in the art at the time of the invention to use the keys of Pennanen in the bitcoin system of Case in order to authenticate the cryptocurrency (Pennanen, paragraph 51).

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.

PCT/US2016/024776

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of:

Regarding Claim 16, Case teaches providing an interface for presentation to individuals via associated computing platforms (paragraph 58 for using a server and the internet with one or more processors and a memory to verify the receiver address for the bitcoins), the interface being configured to allow a verification addresses assigned to the given individual so long as at least one verification address is assigned to the given individual (paragraph 58 for having a user account server that stores information associated with the user's account by matching the scanned fingerprint against the user's stored fingerprint). Case does not explicitly disclose to add or delete verification addresses assigned to the given individual so long as at least one verification address is given. Pennanen has a system for implementing at least one cryptocurrency transaction at a point-of-sale by using a mobile terminal (abstract) and discloses to add or delete verification addresses assigned to the given individual so long as at least one verification address is given (figure 2 for having a user interface for entering a pay to address element 208 with paragraph 68 for having a user interface for facilitating bitcoin transactions and paragraph 51 for having a means to delete keys once a currency has been authenticated). It would have been obvious to one of ordinary skill in the art at the time of the invention to use the keys of Pennanen in the bitcoin system of Case in order to authenticate the cryptocurrency (Pennanen, paragraph 51).

Claims 1-20 meet the criteria set out in PCT Article 33(4), and thus have industrial applicability because the subject matter claimed can be made or used in industry.

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To: IAN C. SCHICK, PH.D.
PILLSBURY WINTHROP SHAW PITTMAN LLP
P.O. BOX 10500
MCLEAN, VA 22102

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43bis.1)

Date of mailing
(day/month/year)

16 JUN 2016

Applicant's or agent's file reference
38918-446543

FOR FURTHER ACTION

See paragraph 2 below

International application No.

PCT/US2016/024776

International filing date (day/month/year)

29 March 2016

Priority date (day/month/year)

28 March 2016

International Patent Classification (IPC) or both national classification and IPC

IPC(8) - G06F 17/30; G06Q 20/36; G06Q 20/38 (2016.01)

CPC - G06Q 20/10; G06Q 20/40; G06Q 40/00 (2016.02)

Applicant

BLACK GOLD COIN, INC.

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step and industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. FURTHER ACTION

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1bis(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA/
Mail Stop PCT, Attn: ISA/US
Commissioner for Patents
P.O. Box 1450, Alexandria, VA 22313-1450
Facsimile No. 571-273-8300

Date of completion of this opinion

22 May 2016

Authorized officer

Blaine R. Copenheaver

PCT Helpdesk: 571-272-4300
PCT OSP: 571-272-7774

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.

PCT/US2016/024776

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:
 - ☒ the international application in the language in which it was filed.
 - ☐ a translation of the international application into _____ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).
2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a)).
3. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing:
 - a. ☐ forming part of the international application as filed:
 - ☐ in the form of an Annex C/ST.25 text file.
 - ☐ on paper or in the form of an image file.
 - b. ☐ furnished together with the international application under PCT Rule 13*ter*.1(a) for the purposes of international search only in the form of an Annex C/ST.25 text file.
 - c. ☐ furnished subsequent to the international filing date for the purposes of international search only:
 - ☐ in the form of an Annex C/ST.25 text file (Rule 13*ter*.1(a)).
 - ☐ on paper or in the form of an image file (Rule 13*ter*.1(b) and Administrative Instructions, Section 713).
4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that forming part of the application as filed or does not go beyond the application as filed, as appropriate, were furnished.
5. Additional comments:

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.

PCT/US2016/024776

Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step and industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	4, 16	YES
	Claims	1-3, 5-15, 17-20	NO
Inventive step (IS)	Claims	None	YES
	Claims	1-20	NO
Industrial applicability (IA)	Claims	1-20	YES
	Claims	None	NO

2. Citations and explanations:

Claims 1-3, 5-15, and 17-20 lack novelty under PCT Article 33(2) as being anticipated by Case Wallet Inc (hereinafter Case).

Regarding Claim 1, Case discloses a system for providing block chain-based multifactor personal identity verification (paragraph 94 for having a bitcoin verification system using a virtual wallet with a multifactor identification system with the factions of a private key, a public key, and a fingerprint, with paragraph 59 for using bitcoins on a block chain ledger; paragraph 83 for multifactor authentication, virtual wallet), the system comprising: one or more hardware processors configured by machine-readable instructions to (paragraph 58 for using a server and the internet with one or more processors and a memory to verify the receiver address for the bitcoins): establish verification addresses on a block chain by (paragraph 58 for verifying the receiver address and amount using the block card to validate a bitcoin transaction; also see paragraph 0059 for block chain): associating identifiers with individuals having previously verified personal identities (paragraph 60 for the user providing identifying information to authorize the use of encryption keys and paragraph 98 for having an initial registration with an email, and phone verification for the user or a previously verified personal identity), a first identifier being associated a first individual (paragraph 59 for getting a first identifier or a private encryption key with a block chain ledger and therefore a first bitcoin address, with paragraph 98 for verifying a user or first individual using a first identifier such as a public key and password salt to ensure the password works with the user's account), the first individual having a previously verified personal identity (paragraph 51 for using fingerprints and biometrics to ensure that only verified users are able to carryout a transaction and paragraph 98 for having an initial user setup process that includes verifying the email and phone to link to a secure device); assigning verification addresses on a block chain to the individuals (paragraph 59 for using a block chain ledger that generates a private encryption key and generating addresses on three branches for receiving bitcoins, buying bitcoins and unspent portions of transactions with three randomly generated encryption keys or verification means), a given verification address including a public key and a private key (paragraph 59 for getting a first identifier or a private encryption key with a block chain ledger and therefore a first bitcoin address with paragraph 94 for having a bitcoin verification system using a virtual wallet with a multifactor identification system with the factions of a private key, a public key, and a fingerprint), a first verification address being assigned to the first individual (paragraph 59 for getting a first identifier or a private encryption key with a block chain ledger and therefore a first bitcoin address with a private key for the first individual), the first verification address including a first public key and a first private key (paragraph 59 for getting a first identifier or a private encryption key with a block chain ledger and therefore a first bitcoin address including a private encryption key and three public encryption keys); and recording identifiers and biometric data associated with the individuals at corresponding verification addresses (paragraph 98 for storing or recording identifiers such as an individuals email and salt passwords or means to record identifiers using a web table as well as identifying a secure device with paragraph 94 for using a private key, a public key, and a fingerprint for the user including the user's browser information), the first identifier and first biometric data associated with the first individual being recorded at the first verification address (paragraph 94 for having a first private key identifier and a first fingerprint biometric data associated with an email or user and paragraph 96 for providing cryptocurrency or bitcoin addresses); and perform block chain-based multifactor personal identity verification using the verification addresses by (paragraph 59 for getting a first identifier or a private encryption key with a block chain ledger and therefore a first bitcoin address): receiving one or more identifiers in connection with one or more requests to verify an identity of one or more individuals (paragraph 68-73 for a user receiving bitcoins by clicking a button or having a request for the bitcoin and then swiping the fingerprint scanner for authentication), the first identifier being received in connection with a request to verify an identity of the first individual (paragraph 59 for getting a first identifier or a private encryption key with a block chain ledger and therefore a first bitcoin address and paragraph 94 for using a fingerprint scanner to authenticate the individual); extracting the biometric data associated with the one or more individuals from the corresponding verification addresses (paragraph 67 for getting fingerprint or biometric data and sending the extracted data to a server for authentication and then completing the transaction based on successful authentication), the first biometric data associated with the first individual being extracted from the first verification address (paragraph 67 for the finger print and the stored encryption key being extracted to the server and verified to complete the transfer of bitcoins to their new owner); 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 (1) biometric data matching the first biometric data (paragraph 57 for providing a third authentication fact such as a fingerprint or biometric data means) and (2) a private key matching the first private key (paragraph 94 for having a bitcoin verification system using a virtual wallet with a multifactor identification system with the factions of a private key, a public key and paragraph 59 for having a private encryption key and three public encryption keys).

Regarding Claim 2, Case discloses wherein the first private key is stored within a computing platform associated with the first individual (paragraph 68 for using a block card element 10 associated with the user along with a fingerprint scanner to send a signed transaction to the server using a wireless transceiver element 368).

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.

PCT/US2016/024776

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of:

Regarding Claim 3, Case 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 (paragraph 59 for using a block chain ledger that generates a private encryption key and generating addresses on three branches for receiving bitcoins, buying bitcoins and unspent portions of transactions with three randomly generated encryption keys or verification means along with a private key for the individual to segregate transactions).

Regarding Claim 5, Case 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 (paragraph 94 for having a first private key identifier and a first fingerprint biometric data associated with an email or user and paragraph 96 for providing cryptocurrency or bitcoin addresses), the first identifier and second biometric data associated with the first individual is recorded at the second verification address (paragraph 84 for having multi-signature address generation with multiple keys stored on different servers or second verification addresses on different servers and secure devices to provide additional security).

Regarding Claim 6, Case 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 (paragraph 90 for using a fingerprint scanner to provide authorization information for a secure transaction and paragraph 51 for using multiple biometric readers such as retina, heart rate, for user verification) and (2) a private key matching the first private key (paragraph 94 for having a bitcoin verification system using a virtual wallet with a multifactor identification system with the factions of a private key, a public key and paragraph 59 for having a private encryption key and three public encryption keys).

Regarding Claim 7, Case discloses wherein the biometric data includes one or more of an image, a recording, or a template (paragraph 90 for using a fingerprint scanner to provide authorization information for a secure transaction and paragraph 51 for using multiple biometric readers such as retina, heart rate, for user verification using a scanner or image means for verification).

Regarding Claim 8, Case 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 (paragraph 90 for using a fingerprint scanner to provide authorization information for a secure transaction and paragraph 51 for using multiple biometric readers such as retina, heart rate, for user verification).

Regarding Claim 9, Case discloses wherein the first biometric data is received via a computing platform associated with the first individual (paragraph 68 for using a block card element 10 associated with the user along with a fingerprint scanner to send a signed transaction to the server using a wireless transceiver element 368).

Regarding Claim 10, Case discloses wherein the one or more hardware processors are further configured by machine-readable instructions to (paragraph 58 for using a server and the internet with one or more processors and a memory to verify the receiver address for the bitcoins), responsive to receiving the request to verify the identity of the first individual (paragraph 59 for getting a first identifier or a private encryption key with a block chain ledger and therefore a first bitcoin address and paragraph 94 for using a fingerprint scanner to authenticate the individual), prompt the first individual for biometric data matching the first biometric data and a private key matching the first private key (paragraph 55 for using a block card with input from the user using control buttons for entering the amount of bitcoins to buy and paragraph 57 for the user logging in as the web portal with an encrypted security key as an authentication factor), the prompt being conveyed via a computing platform associated with the first individual (paragraph 57 for using a web portal as a computing platform and a block card associated with the first individual with figure 3 for having a computer platform with means to prompt a user with a menu).

Regarding Claim 11, Case discloses wherein the one or more hardware processors are further configured by machine-readable instructions to (paragraph 58 for using a server and the internet with one or more processors and a memory to verify the receiver address for the bitcoins), responsive to receiving the request to verify the identity of the first individual (paragraph 59 for getting a first identifier or a private encryption key with a block chain ledger and therefore a first bitcoin address and paragraph 94 for using a fingerprint scanner to authenticate the 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 (paragraph 94 for having a bitcoin verification system using a virtual wallet with a multifactor identification system with the factions of a private key, a public key and paragraph 59 for having a private encryption key and three public encryption keys).

Regarding Claim 12, Case 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 (paragraph 21 for having the biometric data or the fingerprint scan match and a first private key to the server where the server matches a second key stored on the server to broadcast a bitcoin transaction with paragraph 51 for having user verification mechanisms so that only authorized users are able to carryout a transaction).

Regarding Claim 13, Case discloses wherein at least one dedicated node performs the signing of the verification of the personal identity of the first individual (paragraph 52 for having a server or node communicating with a transceiver chip for a partially signed bitcoin transaction).

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.

PCT/US2016/024776

Supplemental Box

In case the space in any of the preceding boxes is not sufficient:

Continuation of:

Regarding Claim 14, Case teaches a method for establishing verification addresses on a block chain in order to provide block chain-based multifactor personal identity verification (paragraph 94 for having a bitcoin verification system using a virtual wallet with a multifactor identification system with the factions of a private key, a public key, and a fingerprint, with paragraph 59 for using bitcoins on a block chain ledger; paragraph 83 for multifactor authentication, virtual wallet), the method being performed by one or more hardware processors configured by machine-readable instructions (paragraph 58 for using a server and the internet with one or more processors and a memory to verify the receiver address for the bitcoins), the method comprising: associating identifiers with individuals having previously verified personal identities (paragraph 60 for the user providing identifying information to authorize the use of encryption keys and paragraph 98 for having an initial registration with an email, and phone verification for the user or a previously verified personal identity, with paragraph 59 for getting a first identifier or a private encryption key with a block chain ledger and therefore a first bitcoin address), a first identifier being associated a first individual, the first individual having a previously verified personal identity (paragraph 51 for using fingerprints and biometrics to ensure that only verified users are able to carryout a transaction and paragraph 98 for having an initial user setup process that includes verifying the email and phone to link to a secure device); assigning verification addresses on a block chain to the individuals (paragraph 59 for using a block chain ledger that generates a private encryption key and generating addresses on three branches for receiving bitcoins, buying bitcoins and unspent portions of transactions with three randomly generated encryption keys or verification means), a given verification address including a public key and a private key (paragraph 59 for getting a first identifier or a private encryption key with a block chain ledger and therefore a first bitcoin address with paragraph 94 for having a bitcoin verification system using a virtual wallet with a multifactor identification system with the factions of a private key, a public key, and a fingerprint), a first verification address being assigned to the first individual (paragraph 59 for getting a first identifier or a private encryption key with a block chain ledger and therefore a first bitcoin address with a private key for the first individual), the first verification address including a first public key and a first private key (paragraph 59 for getting a first identifier or a private encryption key with a block chain ledger and therefore a first bitcoin address including a private encryption key and three public encryption keys); and recording identifiers and biometric data associated with the individuals at corresponding verification addresses (paragraph 98 for storing or recording identifiers such as an individuals email and salt passwords or means to record identifiers using a web table as well as identifying a secure device with paragraph 94 for using a private key, a public key, and a fingerprint for the user including the user's browser information), the first identifier and first biometric data associated with the first individual being recorded at the first verification address (paragraph 59 for getting a first identifier or a private encryption key with a block chain ledger and therefore a first bitcoin address with paragraph 94 for having a bitcoin verification system using a virtual wallet with a multifactor identification system with the factions of a private key, a public key, and a fingerprint); wherein the identity of the one or more individuals are verifiable upon receiving matching biometric data and private keys (paragraph 67 for the finger print and the stored encryption key being extracted to the server and verified to complete the transfer of bitcoins to their new owner), the personal identity of the first individual being verifiable upon receipt of (1) biometric data matching the first biometric data (paragraph 57 for providing a third authentication fact such as a fingerprint or biometric data means) and (2) a private key matching the first private key (paragraph 94 for having a bitcoin verification system using a virtual wallet with a multifactor identification system with the factions of a private key, a public key and paragraph 59 for having a private encryption key and three public encryption keys).

Regarding Claim 15, Case teaches assigning multiple verification addresses to separate individuals such that, in addition to the first verification address, a second verification address is assigned to the first individual (paragraph 59 for using a block chain ledger that generates a private encryption key and generating addresses on three branches for receiving bitcoins, buying bitcoins and unspent portions of transactions with three randomly generated encryption keys or verification means along with a private key for the individual to segregate transactions).

Regarding Claim 17, Case teaches recording different biometric data 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 (paragraph 94 for having a first private key identifier and a first fingerprint biometric data associated with an email or user and paragraph 96 for providing cryptocurrency or bitcoin addresses), the first identifier and second biometric data associated with the first individual is recorded at the second verification address (paragraph 84 for having multi-signature address generation with multiple keys stored on different servers or second verification addresses on different servers and secure devices to provide additional security).

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.

PCT/US2016/024776

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of:

Regarding Claim 18, Case teaches method for perform block chain-based multifactor personal identity verification using verification addresses (paragraph 94 for having a bitcoin verification system using a virtual wallet with a multifactor identification system with the factions of a private key, a public key, and a fingerprint, with paragraph 59 for using bitcoins on a block chain ledger; paragraph 83 for multifactor authentication, virtual wallet), the method being performed by one or more hardware processors configured by machine-readable instructions (paragraph 58 for using a server and the internet with one or more processors and a memory to verify the receiver address for the bitcoins), the method comprising: receiving one or more identifiers in connection with one or more requests to verify an identity of one or more individuals (paragraph 60 for the user providing identifying information to authorize the use of encryption keys and paragraph 98 for having an initial registration with an email, and phone verification for the user or a previously verified personal identity, with paragraph 59 for getting a first identifier or a private encryption key with a block chain ledger and therefore a first bitcoin address), a first identifier being received in connection with a request to verify an identity of a first individual (paragraph 51 for using fingerprints and biometrics to ensure that only verified users are able to carryout a transaction and paragraph 98 for having an initial user setup process that includes verifying the email and phone to link to a secure device); extracting biometric data associated with the one or more individuals from corresponding verification addresses on a block chain (paragraph 59 for using a block chain ledger that generates a private encryption key and generating addresses on three branches for receiving bitcoins, buying bitcoins and unspent portions of transactions with three randomly generated encryption keys or verification means), a given verification address including a public key and a private key (paragraph 59 for getting a first identifier or a private encryption key with a block chain ledger and therefore a first bitcoin address with paragraph 94 for having a bitcoin verification system using a virtual wallet with a multifactor identification system with the factions of a private key, a public key, and a fingerprint), first biometric data associated with the first individual being extracted from a first verification address assigned to the first individual (paragraph 59 for getting a first identifier or a private encryption key with a block chain ledger and therefore a first bitcoin address with a private key for the first individual), the first verification address including a first public key and a first private key (paragraph 59 for getting a first identifier or a private encryption key with a block chain ledger and therefore a first bitcoin address including a private encryption key and three public encryption keys); and verifying the identity of the one or more individuals upon receiving matching biometric data and private keys (paragraph 67 for the finger print and the stored encryption key being extracted to the server and verified to complete the transfer of bitcoins to their new owner) the personal identity of the first individual being verified upon receipt of (1) biometric data matching the first biometric data (paragraph 57 for providing a third authentication fact such as a fingerprint or biometric data means) and (2) a private key matching the first private key (paragraph 94 for having a bitcoin verification system using a virtual wallet with a multifactor identification system with the factions of a private key, a public key and paragraph 59 for having a private encryption key and three public encryption keys).

Regarding Claim 19, Case teaches responsive to receiving the request to verify the identity of the first individual (paragraph 58 for using a server and the internet with one or more processors and a memory to verify the receiver address for the bitcoins), responsive to receiving the request to verify the identity of the first individual (paragraph 59 for getting a first identifier or a private encryption key with a block chain ledger and therefore a first bitcoin address and paragraph 94 for using a fingerprint scanner to authenticate the individual); prompting the first individual for biometric data matching the first biometric data and a private key matching the first private key (paragraph 55 for using a block card with input from the user using control buttons for entering the amount of bitcoins to buy and paragraph 57 for the user logging in as the web portal with an encrypted security key as an authentication factor), the prompt being conveyed via a computing platform associated with the first individual (paragraph 57 for using a web portal as a computing platform and a block card associated with the first individual with figure 3 for having a computer platform with means to prompt a user with a menu); 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 (paragraph 94 for having a bitcoin verification system using a virtual wallet with a multifactor identification system with the factions of a private key, a public key and paragraph 59 for having a private encryption key and three public encryption keys).

Regarding Claim 20, Case teaches 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 (paragraph 21 for having the biometric data or the fingerprint scan match and a first private key to the server where the server matches a second key stored on the server to broadcast a bitcoin transaction with paragraph 51 for having user verification mechanisms so that only authorized users are able to carryout a transaction).

Claims 4 and 16 lack an inventive step under PCT Article 33(3) as being obvious over Case Wallet Inc (hereinafter Case) in view of Pennanen.

Regarding Claim 4, Case 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 (paragraph 58 for using a server and the internet with one or more processors and a memory to verify the receiver address for the bitcoins), the interface being configured to allow a given individual for a verification address is assigned to the given individual (paragraph 58 for having a user account server that stores information associated with the user's account by matching the scanned fingerprint against the user's stored fingerprint). Case does not explicitly disclose to add or delete verification addresses assigned to the given individual so long as at least one verification address is given. Pennanen has a system for implementing at least one cryptocurrency transaction at a point-of-sale by using a mobile terminal (abstract) and discloses to add or delete verification addresses assigned to the given individual so long as at least one verification address is given (figure 2 for having a user interface for entering a pay to address element 208 with paragraph 68 for having a user interface for facilitating bitcoin transactions and paragraph 51 for having a means to delete keys once a currency has been authenticated). It would have been obvious to one of ordinary skill in the art at the time of the invention to use the keys of Pennanen in the bitcoin system of Case in order to authenticate the cryptocurrency (Pennanen, paragraph 51).

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.

PCT/US2016/024776

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of:

Regarding Claim 16, Case teaches providing an interface for presentation to individuals via associated computing platforms (paragraph 58 for using a server and the internet with one or more processors and a memory to verify the receiver address for the bitcoins), the interface being configured to allow a verification addresses assigned to the given individual so long as at least one verification address is assigned to the given individual (paragraph 58 for having a user account server that stores information associated with the user's account by matching the scanned fingerprint against the user's stored fingerprint). Case does not explicitly disclose to add or delete verification addresses assigned to the given individual so long as at least one verification address is given. Pennanen has a system for implementing at least one cryptocurrency transaction at a point-of-sale by using a mobile terminal (abstract) and discloses to add or delete verification addresses assigned to the given individual so long as at least one verification address is given (figure 2 for having a user interface for entering a pay to address element 208 with paragraph 68 for having a user interface for facilitating bitcoin transactions and paragraph 51 for having a means to delete keys once a currency has been authenticated). It would have been obvious to one of ordinary skill in the art at the time of the invention to use the keys of Pennanen in the bitcoin system of Case in order to authenticate the cryptocurrency (Pennanen, paragraph 51).

Claims 1-20 meet the criteria set out in PCT Article 33(4), and thus have industrial applicability because the subject matter claimed can be made or used in industry.



(51) International Patent Classification:

G06F 17/30 (2006.01) G06Q 20/38 (2012.01)
G06Q 20/36 (2012.01)

(21) International Application Number:

PCT/US2016/024776

(22) International Filing Date:

29 March 2016 (29.03.2016)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

15/083,241 28 March 2016 (28.03.2016) US

(71) Applicant: **BLACK GOLD COIN, INC.** [US/US]; 7495
Azure Drive, Suite 100, Las Vegas, Nevada 89130 (US).

(72) Inventor: **ANDRADE, Marcus**; 564 Wedge Lane, Fern-
ley, Nevada 89408 (US).

(74) Agents: **SCHICK, PH.D., Ian C.** et al.; PILLSBURY
WINTHROP SHAW PITTMAN LLP, P.O. Box 10500,
McLean, Virginia 22102 (US).

(81) Designated States (unless otherwise indicated, for every
kind of national protection available): AE, AG, AL, AM,
AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY,
BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM,
DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT,
HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR,
KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG,
MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM,
PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC,
SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN,
TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every
kind of regional protection available): ARIPO (BW, GH,
GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ,
TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU,
TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE,
DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU,
LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK,
SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ,
GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— with international search report (Art. 21(3))

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

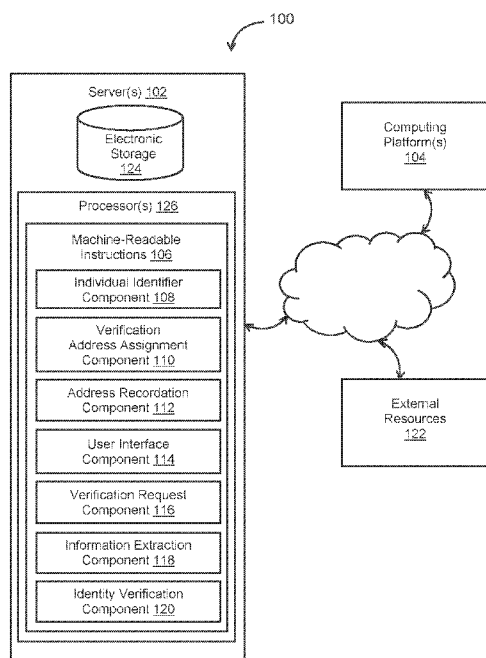


FIG. 1

(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.

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

FIELD OF THE DISCLOSURE

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

SUMMARY

(02) 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.

(03) 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.

(04) 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.

(05) 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

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

(07) 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.

(08) 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

(09) 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 architecture,

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

(10) 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.

(11) 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.

(12) 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.

(13) 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.

(14) 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."

(15) 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.

(16) 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.

(17) 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.

(18) 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.

(19) 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.

(20) 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.

(21) 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.

(22) 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.

(23) 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.

(24) 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.

(25) 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.

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

(27) 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.

(28) 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.

(29) 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.

(30) 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.

(31) 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.

(32) 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.

(33) 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.

(34) 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.

(35) 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.

(36) 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.

(37) 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.

(38) 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.

(39) 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.

(40) 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.

(41) 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.

(42) 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.

(43) 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.

(44) 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 configured through hardware, firmware, and/or software to be specifically designed for execution of one or more of the operations of method 200.

(45) 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.

(46) 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.

(47) 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.

(48) 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.

(49) 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.

(50) 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.

(51) 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.

(52) 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.

(53) 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.

(54) 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.

(55) 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.

(56) 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 block chain-based multifactor personal identity verification, the system comprising:
 - one or more hardware processors configured by machine-readable instructions to:
 - 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;
 - 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; and
 - perform block chain-based multifactor personal identity verification using the verification addresses 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;

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.

2. The system of claim 1, wherein the first private key is stored within a computing platform associated with the first individual.
3. The system of claim 1, 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.
4. The system of claim 1, 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, 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.

5. The system of claim 1, 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.
6. The system of claim 5, 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.
7. The system of claim 1, wherein the biometric data includes one or more of an image, a recording, or a template.
8. The system of claim 1, 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.
9. The system of claim 1, wherein the first biometric data is received via a computing platform associated with the first individual.
10. The system of claim 1, 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 data and a private key matching the first private key, the prompt being conveyed via a computing platform associated with the first individual.

11. The system of claim 1, 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.
12. The system of claim 1, 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.
13. The system of claim 1, wherein at least one dedicated node performs the signing of the verification of the personal identity of the first individual.
14. A method for establishing verification addresses on a block chain in order to provide block chain-based multifactor personal identity verification, the method being performed by one or more hardware processors configured by machine-readable instructions, the method comprising:

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;

wherein the identity of the one or more individuals are verifiable upon receiving matching biometric data and private keys, the personal identity of the first individual being verifiable upon receipt of (1) biometric data matching the first biometric data and (2) a private key matching the first private key.

15. The method of claim 14, further comprising assigning multiple verification addresses to separate individuals such that, in addition to the first verification address, a second verification address is assigned to the first individual.
16. The method of claim 14, further comprising providing an interface for presentation to individuals via associated computing platforms, 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.

17. The method of claim 14, further comprising recording different biometric data 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.
18. A method for perform block chain-based multifactor personal identity verification using verification addresses, the method being performed by one or more hardware processors configured by machine-readable instructions, the method comprising:
 - 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.

19. The method of claim 18, further comprising, 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;
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.

20. The method of claim 18, 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.

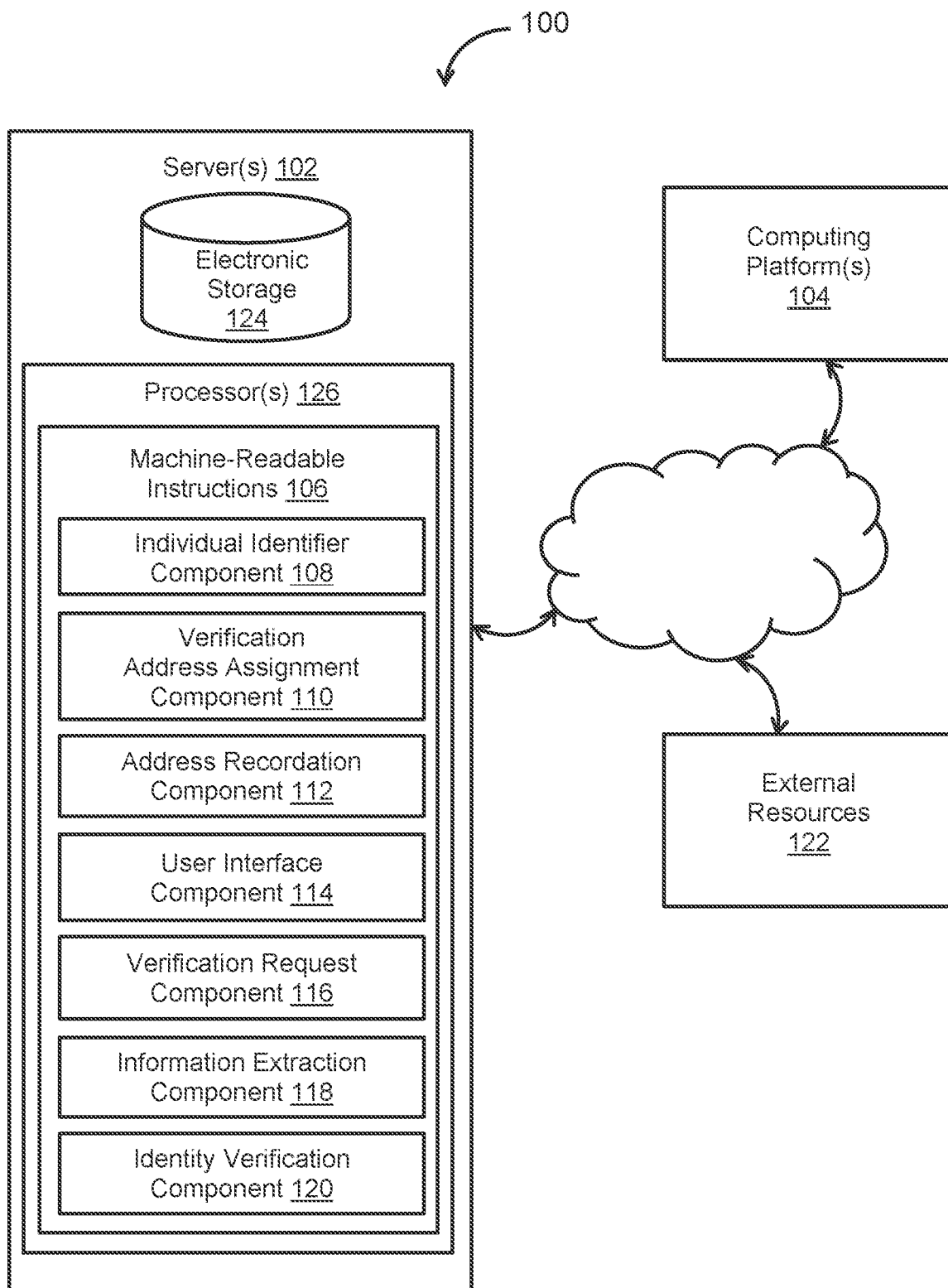


FIG. 1

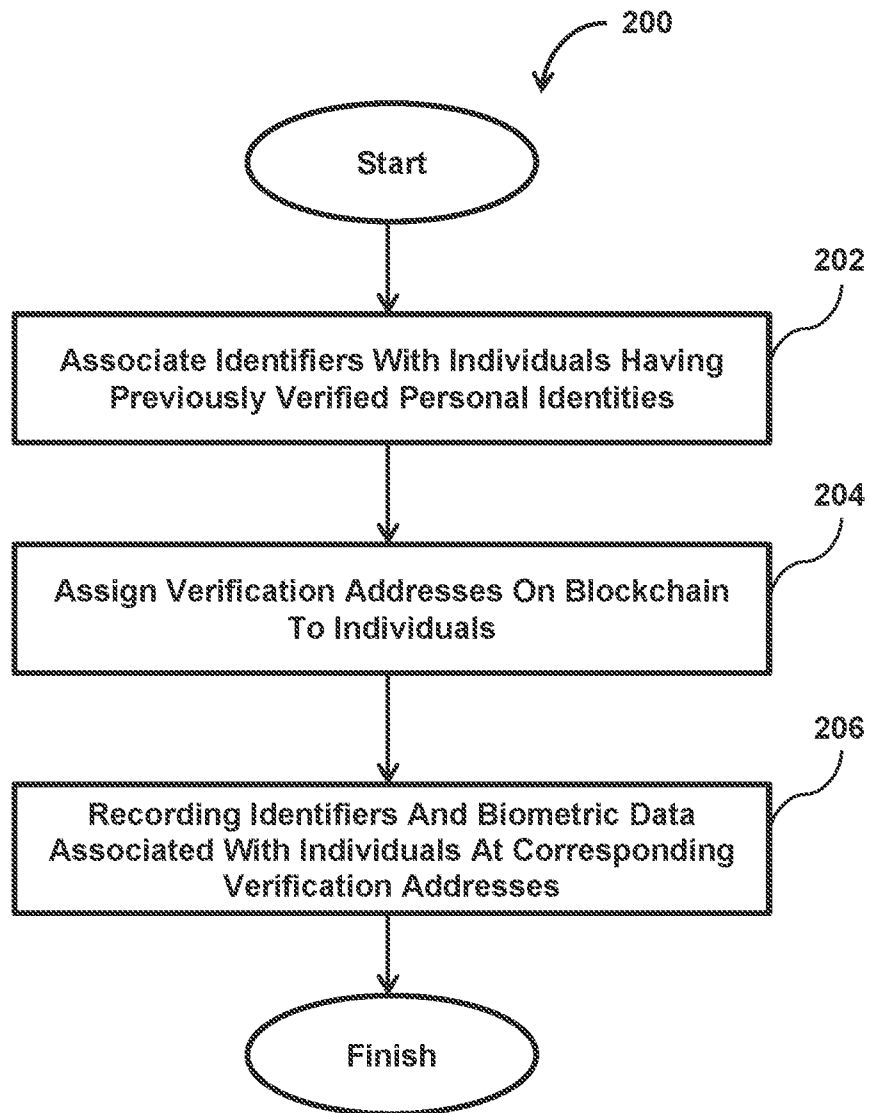


FIG. 2

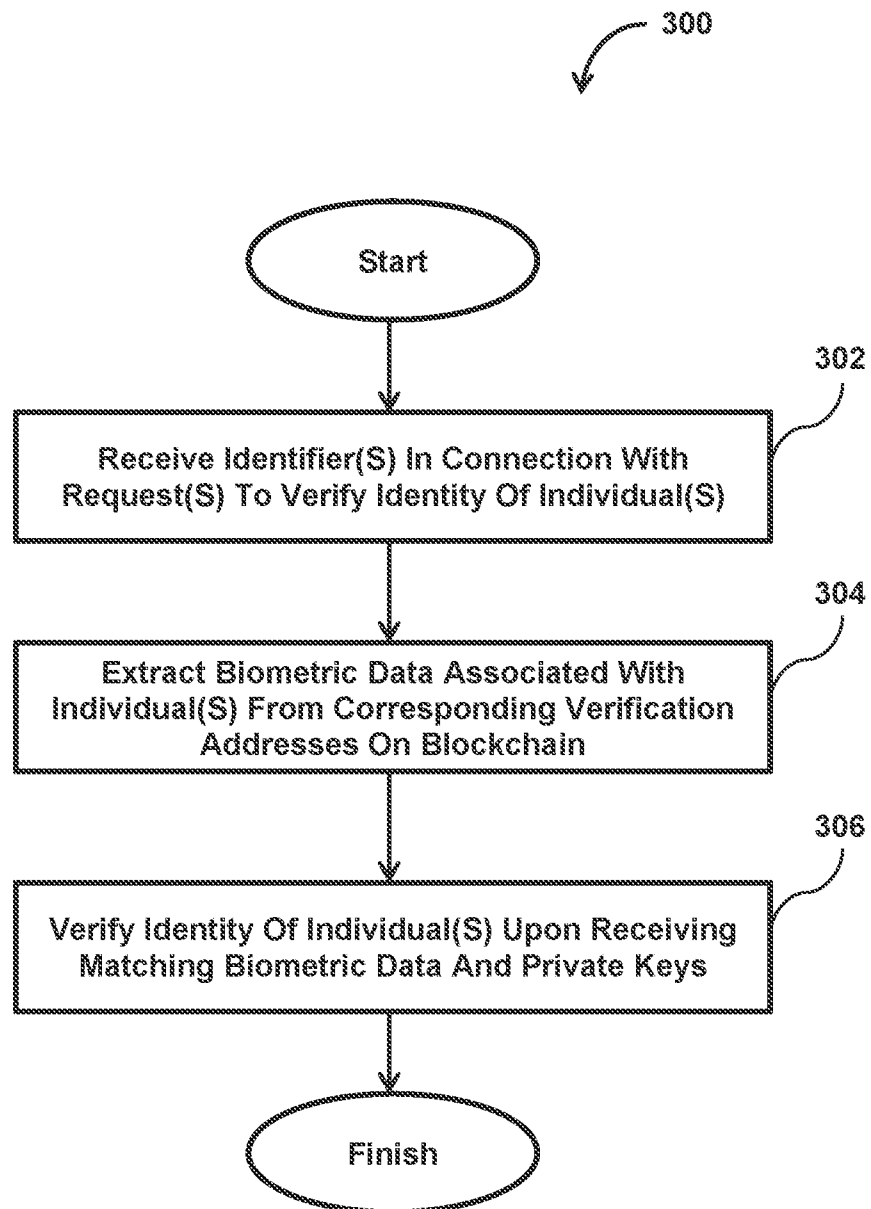


FIG. 3

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US2016/024776

A. CLASSIFICATION OF SUBJECT MATTER

IPC(8) - G06F 17/30; G06Q 20/36; G06Q 20/38 (2016.01)

CPC - G06Q 20/10; G06Q 20/40; G06Q 40/00 (2016.02)

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC(8) - G06F 17/30; G06Q 20/36; G06Q 20/38 (2016.01)

CPC - G06Q 20/10; G06Q 20/40; G06Q 40/00 (2016.02)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

USPC - 705/44; 713/168; 726/5 (keyword delimited)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Orbit, Google Patents, Google

Search terms used: bitcoin, block, chain, multi-factor, authentication, biometric, authenticate

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2015/0324789 A1 (CASE WALLET INC) 12 November 2015 (12.11.2015) entire document	1-3, 5-15, 17-20
---		---
Y		4, 16
Y	US 2015/0356555 A1 (PENANEN) 10 December 2015 (10.12.2015) entire document	4, 16
A	US 2012/0084563 A1 (SINGHAL) 05 April 2012 (05.04.2012) entire document	1-20
A	US 2015/0178693 A1 (SOLIS) 25 June 2015 (25.06.2015) entire document	1-20

☐ Further documents are listed in the continuation of Box C.☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

22 May 2016

Date of mailing of the international search report

16 JUN 2016

Name and mailing address of the ISA/

Mail Stop PCT, Attn: ISA/US, Commissioner for Patents

P.O. Box 1450, Alexandria, VA 22313-1450

Facsimile No. 571-273-8300

Authorized officer

Blaine R. Copenheaver

PCT Helpdesk: 571-272-4300

PCT OSP: 571-272-7774