US Patent & Trademark Office
Patent Public Search | Text View

United States Patent	12388809
Kind Code	B2
Date of Patent	August 12, 2025
Inventor(s)	Weimer; Jonathan et al.

Blockchain systems and methods for user authentication

Abstract

Computer-implemented methods and systems are provided for blockchain-mediated user authentication. Consistent with disclosed embodiments, authentication may comprise operations including receiving, from a user system, an authentication request for a user. The operations may also include determining a root system for the user using a blockchain, and redirecting the user system to the root system. The operations may include receiving, following redirection, a verification message indicating that the root system successfully authenticated the user, and including an authorization code for receiving, from the root system, a root system secret. The operations may include receiving from a database, identification data using the root system secret. Determining the root system may comprise identifying, using the authentication request and index information stored in the blockchain, a block of the blockchain storing root system information for the user. Receiving the identification data may comprise retrieving identification data from the database.

Inventors:	**Weimer; Jonathan (Henrico, VA), Fox; Ryan (Alexandria, VA)**
Applicant:	**Capital One Services, LLC** (McLean, VA)
Family ID:	**60660445**
Assignee:	**Capital One Services, LLC (McLean, VA)**
Appl. No.:	**18/310506**
Filed:	**May 01, 2023**

Prior Publication Data

Document Identifier	Publication Date
US 20230275884 A1	Aug. 31, 2023

Related U.S. Application Data

continuation parent-doc US 17195194 20210308 US 11665147 child-doc US 18310506
continuation parent-doc US 16293796 20190306 US 10944563 20210309 child-doc US 17195194
continuation parent-doc US 15839530 20171212 US 10277398 20190430 child-doc US 16293796
continuation parent-doc US 15626054 20170616 US 10454683 20191022 child-doc US 15839530
us-provisional-application US 62351894 20160617

Publication Classification

Int. Cl.: **H04L9/40** (20220101); **G06F21/31** (20130101); **H04L9/32** (20060101); H04L9/00 (20220101)

U.S. Cl.:

CPC **H04L63/08** (20130101); **G06F21/31** (20130101); **H04L9/3213** (20130101); **H04L9/3239** (20130101); H04L9/50 (20220501)

Field of Classification Search

CPC: G06F (21/31); H04L (9/321-3213); H04L (9/3236-3242); H04L (9/50); H04L (63/08)

References Cited

U.S. PATENT DOCUMENTS

Patent No.	Issued Date	Patentee Name	U.S. Cl.	CPC
8949269	12/2014	Wolff	707/769	G06Q 10/10
2017/0180128	12/2016	Lu	N/A	H04L 9/3239
2017/0257358	12/2016	Ebrahimi	N/A	H04L 9/3236

Primary Examiner: Bechtel; Kevin

Attorney, Agent or Firm: Foley & Lardner LLP

Background/Summary

CROSS-REFERENCE TO RELATED APPLICATIONS (1) This application is a continuation of U.S. patent application Ser. No. 17/195,194, filed Mar. 8, 2021, which is a continuation of U.S. patent application Ser. No. 16/293,796, filed Mar. 6, 2019, which is a continuation of U.S. patent application Ser. No. 15/839,530, filed Dec. 12, 2017, which is a continuation of U.S. patent application Ser. No. 15/626,054, filed Jun. 16, 2017, which claims the benefit of priority of U.S. Provisional Application No. 62/351,894, filed Jun. 17, 2016, which applications are expressly incorporated herein by reference in their entirety.

TECHNICAL FIELD
(1) The disclosed embodiments concern an authentication system including multiple member systems. More specifically, the disclosed embodiments concern recording authentication information for a user in a blockchain, and enabling members of the authentication system to retrieve user identification data from a database using the authentication information.
BACKGROUND

(2) Users may attempt interactions with computer systems associated with multiple institutions. These institutions may configure their associated computer systems to require authentication of users attempting to access the computer systems. Implementing such authentication requirements can impose time and resource burdens on the institutions. Additionally, users may resent having to respond to repeated authentication requests as they navigate between computer systems associated with different institutions. Institutions and users may therefore benefit from a collaborative authentication system that handles authentication interactions for multiple institutions.

(3) But such collaboration requires overcoming certain technical problems. A preferable authentication system would track authentication interactions for users attempting to access the computer systems of the participating institutions. Such an authentication system would be non-reputable, preventing users or institutions from later challenging authentication records as false or inaccurate. Furthermore, a preferable authentication system would limit sharing of personal information between the users and the institutions. The authentication system would also be constructed in a way that encouraged the participating institutions to trust in the validity of the authentication records. A need therefore exists for an authentication system architecture that addresses these technical problems. The disclosed embodiments provide a specific example of such an authentication system architecture.

SUMMARY

(4) The disclosed embodiments concern an authentication system that maintains a distributed, non-reputable record of authentication interactions, while limiting the sharing of personal information between institutions. This authentication system may be used by multiple participating member systems. Accordingly, as described in greater detail below, this system solves the above-mentioned technical problems with collaborative authentication systems.

(5) In some embodiments, a root system may establish an identity for each user of the authentication system. The root system may store information in a blockchain. This information may enable other members of the authentication system to locate the root system. The root system may also store identification data for the user in a database. Member systems may rely on the root system for authenticate the user, and may interact with the root system to retrieve the stored identification data. The blockchain may provide a distributed, non-reputable record of interactions between the user, the member systems, and the root system.

(6) The disclosed embodiments may include, for example, an authentication system comprising at least one processor; and at least one non-transitory memory. The non-transitory memory may contain instructions that, when executed by the at least one processor, cause the authentication system to perform operations. The operations may comprise receiving, from a user system, an authentication request for a user. The operations may also comprise determining a root system for the user using a blockchain, and redirecting the user system to the root system. The operations may also comprise receiving, from the root system, a root system secret, and receiving, from a database, identification data using the root system secret.

(7) The disclosed embodiments may further include an authentication system comprising at least one processor; and at least one non-transitory memory. The non-transitory memory may contain instructions that, when executed by the at least one processor, cause the authentication system to perform operations. The operations may comprise receiving personal information for a user. The operations may also comprise generating identification data and index information for the user using the received personal information. The operations may additionally comprise writing the root system information and the index information to a blockchain, encrypting the identification data using a root system key; and storing the encrypted identification data in a database.

(8) It is to be understood that both the foregoing general description and the following detailed description are exemplary and explanatory only and are not restrictive of the disclosed embodiments, as claimed.

Description

BRIEF DESCRIPTION OF THE DRAWINGS

(1) The drawings are not necessarily to scale or exhaustive. Instead, emphasis is generally placed upon illustrating the principles of the inventions described herein. The accompanying drawings, which are incorporated in and constitute a part of this specification, illustrate several embodiments consistent with the disclosure and together with the description, serve to explain the principles of the disclosure. In the drawings:

(2) FIG. **1** depicts a schematic of an exemplary system for authenticating users.

(3) FIG. **2** depicts a logical model of an exemplary blockchain.

(4) FIG. **3**A depicts a logical model of a message stored in a blockchain.

(5) FIG. **3**B depicts a logical model of identification data stored in a database.

(6) FIG. **4** depicts an exemplary process for establishing a user identity.

(7) FIG. **5** depicts an exemplary process for authenticating a user.

(8) FIG. **6** depicts exemplary user interfaces for multi-factor authentication.

(9) FIG. **7** depicts a schematic of an exemplary computing device for performing the envisioned systems and methods.

(10) FIG. **8** depicts a flow diagram of an exemplary implementation.

(11) FIG. **9** depicts an exemplary customer verification flow.

(12) FIG. **10** depicts an exemplary sequence of data exchange.

DETAILED DESCRIPTION

(13) Reference will now be made in detail to the disclosed embodiments, examples of which are illustrated in the accompanying drawings. Wherever convenient, the same reference numbers will be used throughout the drawings to refer to the same or like parts.

(14) FIG. **1** depicts a schematic of an exemplary system for authenticating users (authentication system **100**), consistent with disclosed embodiments. Authentication system **100** may comprise systems with access to blockchain **105** and database **109** over network **111**. Authentication system **100** may enable the systems to share user authentication information and responsibility for authenticating users. For each user, as described below, a system may initially authenticate a user. This system becomes the root system for this user (e.g., root system **107**). This system may create a message in blockchain **105** corresponding to the user. This entry may indicate the user, and provide root system information for contacting root system **107**. Root system **107** may also be configured to create an entry in database **109** storing identification data for user. The remaining systems, referred to herein a member system (e.g., member system **103**), may be configured to redirect authentication requests from a user system (e.g., user system **101**) for the user to the root system **107**. The member system may be configured to recover the identification data for the user from database **109**, following authentication of the user by root system **107**. The member system may be configured to document this authentication transaction in blockchain **105**.

(15) The disclosed authentication system can therefore use the root system to securely store personal information. The disclosed authentication system can also generate a non-reputable record of authentication interactions using a blockchain, which can also provide information enabling the participating systems to contact the root system. Furthermore, this blockchain can be distributed, encouraging trust in the validity of the authentication interaction records. In this manner, the disclosed authentication systems provide an innovative technical solution to at least the above-mentioned technical problems with collaborative authentication systems.

(16) As would be recognized by one of skill in the art, the description of authentication system **100** in FIG. **1** is not intended to be limiting. In some embodiments, additional elements may be added, and/or the depicted elements of authentication system **100** may be combined, divided, modified, or removed. For example, envisioned embodiments may implement a superset or a subset of the

depicted elements of authentication system **100**. As an additional example, in some embodiments, at least one of blockchain **105** and database **109** may be implements by another element of authentication system **100** (e.g., member system **103** or root system **107**).

(17) User system **101** may be configured to provide an authentication request, consistent with disclosed embodiments. User system **101** may comprise a computing device, such as a server, workstation, desktop, or mobile device (e.g., laptop, tablet, phablet, smartphone, smartwatch, or similar mobile computing device). As described below with respect to FIG. **7**, user system **101** may be configured with a display and input/output interfaces. User system **101** may be configured to interact with a user (not shown) using the display and input/output interfaces. User system **101** may be configured to contact member system **103** and provide an authentication request for the user, based on this interaction. User system **101** may be configured as an "end-user" in an OpenID framework, as described in "OpenID Authentication 2.0-Final," referred to herein as "OpenID" and hereby incorporated by reference in its entirety.

(18) Member system **103** may be configured to authenticate users, consistent with disclosed embodiments. Member system **103** may include one or more computing devices, such as servers, workstations, desktop computers, or special-purpose computing devices. Member systems (e.g., member system **103**) may act as "relying parties" in an OpenID framework, as described in OpenID and incorporated herein by reference. Member system **103** may be standalone, or it may be part of a subsystem, which may be part of a larger system. For example, member system **103** may be associated with a commercial institution. Member system **103** may include distributed servers that are remotely located and communicate with other systems of the financial institution over a public network, or over a dedicated private network.

(19) Member system **103** may be configured to receive a request to authenticate a user. In some embodiments, member system **103** may be configured to receive the request from another element of authentication system **100**, such as user system **101**, or from another system. Member system **103** may be configured to interact with blockchain **105**, root system **107**, and database **109** to process the authentication request. In some embodiments, processing the authentication request may comprise receiving identification data from database **109**. Member system **103** may be configured to use this identification data to perform a business process. For example, the business process may require customer identification, according to statutory or regulatory guidelines. The receipt of the identification data may satisfy these guidelines. As an additional example, the received identification data may be used to populate forms, expediting the business process and improving the customer experience.

(20) Member system **103** may be configured to store messages in blockchain **105**, consistent with disclosed embodiments. In some aspects, member system **103** may be configured to add blocks containing the messages to blockchain **105**. In various aspects, member system **103** may be configured to provide the messages to an authorized system. The authorized system may be configured to add blocks containing the messages to blockchain **105**. As described below with regards to FIG. **3**A, the messages may comprise index information **303** and authentication records **307**.

(21) Blockchain **105** may comprise a distributed data structure, consistent with disclosed embodiments. Blockchain **105** may be a private blockchain. For example, authorized systems may store copies of blockchain **105**. These authorized systems may be configured to add blocks to blockchain **105** and publish the blocks to other authorized systems. Authorized systems may be configured to receive messages from other systems for publication in blockchain **105**. These other systems may have read-only access to blockchain **105**. In some embodiments, at least one of member system **103** and root system **107** are authorized systems. In various embodiments, member system **103** and root system **107** may not be authorized systems. As described in detail with respect to FIG. **3**A, blockchain **105** may be configured to store messages from member systems including authentication records **307**.

(22) Root system **107** may be configured to authenticate users, consistent with disclosed embodiments. Root system **107** may include one or more computing devices, such as servers, workstations, desktop computers, or special-purpose computing devices. In some embodiments, root system **107** may be associated with an OpenID connect endpoint. As would be understood by one of skill in the art, the OpenID connect endpoint may enable the root system **107** to serve as an identify provider. Root system **107** may be standalone, or it may be part of a subsystem, which may be part of a larger system. For example, root system **107** may be associated with a commercial institution. Root system **107** may include distributed servers that are remotely located and communicate with other systems of the financial institution over a public network, or over a dedicated private network. Root system **107** may be configured to receive a request to authenticate a user. In some embodiments, root system **107** may be configured to receive the request from another element of authentication system **100**, such as user system **101**, or from another system.

(23) Database **109** may be configured to store identification data for the user, consistent with disclosed embodiments. In some aspects, database **109** may comprise a distributed database. For example, database **109** may comprise a federated database. As an additional example, database **109** may comprise a distributed hash table. In some aspects, nodes of this distributed hash table may be associated with members of authentication system **100** (e.g., member system **103** and root system **107**).

(24) Network **111** may be configured to provide communications between components of FIG. **1**. For example, network **111** may be any type of network (including infrastructure) that provides communications, exchanges information, and/or facilitates the exchange of information, such as the Internet, a Local Area Network, or other suitable connection(s) that enables authentication system **100** to send and receive information between the components of authentication system **100**.

(25) FIG. **2** depicts a logical model of an exemplary blockchain, consistent with disclosed embodiments. Blockchain **105** may comprise many such blockchains maintained by many different systems (e.g., member system **103**, root system **107**, or other systems). Such exemplary blockchains may comprise blocks, such as blocks **201***a*-**201***d*. Blocks may include messages, such as message **207***b* and message **207***d*. Blocks may include a header, such as header **202***b*. The header may include at least one of the previous block's hash (e.g., hash **203***b*), a hash of any messages in the block (e.g., a Merkle root) and a timestamp. Consistent with disclosed embodiments, authentication system **100** may require that blocks added to blockchain **105** satisfy at least one of a proof-of-work condition and a digital signature condition. For example, the header may include a nonce chosen to ensure the header satisfies the proof-of-work condition. As a non-limiting example, the proof-of-work condition may require the hash of the header fall within a predetermined range of values. As an additional example, the header may be digitally signed with a cryptographic key of an authorized system, and the digital signature may be included in the header. This digital signature may be verified using a key available to the members of authentication system **100**.

(26) FIG. **3**A depicts a logical model of a message **207***b* stored in a blockchain (e.g., an element of blockchain **105**), consistent with disclosed embodiments. In some embodiments, message **207***b* may comprise index information **303**. In certain aspects, index information **303** may comprise information identifying a user. For example, index information **303** may be at least one of a full name, email address, phone number, or other non-sensitive personal information of the user. In various aspects, index information **303** may include one or more references to earlier blocks in the private blockchain. For example, index information **303** may include one or more references to one or more earlier blocks associated with the same user. A reference may include, as a non-limiting example, a hash of a preceding block in the blockchain associated with the same user. In some aspects, index information **303** may be obfuscated or encrypted according to methods known to one of skill in the art. For example, index information **303** may be encrypted with a cryptographic key. As an additional example, index information **303** may comprise a hash of the at least one of a full

name, email address, phone number, or other non-sensitive personal information of the user.

(27) Message **207***b* may comprise root system information **305**, consistent with disclosed embodiments. In some aspects, root system information **305** may indicate a location associated with root system **107**. For example, root system information **305** may comprise a Uniform Resource Identifier (URI), such as a Uniform Resource Locator (URL) for root system **107**. As an additional example, root system information **305** may comprise an Extensible Resource Identifier (XRI) for root system **107**, as described in OpenID and incorporated herein by reference. As an additional example, root system information **305** may comprise a name or token, such as a uniform resource name (URN). In some aspects, a member of authentication system **100** may be configured to use root system information **305** to retrieve a URI or XRI for root system **107**. For example, the URI and/or XRI may indicate the location of a service that, in turn, provides the location of root system **107**. As an additional example, a translation service hosted by an element of authentication system **100**, or another system, may translate the name or token into a location of root system **107**. In various aspects, root system information **305** may be obfuscated or encrypted according to methods known to one of skill in the art. For example, root system information **305** may be encrypted with a cryptographic key.

(28) Message **207***b* may comprise authentication record **307**, consistent with disclosed embodiments. In some aspects, authentication record **307** may comprise information enabling subsequent auditing of transactions. For example, authentication record **307** may identify at least one of member system **103**, a commercial institution associated with member system **103**, root system **107**, a commercial institution associated with root system **107**, a purpose of the authentication request, a result of the authentication request, and information related to the authentication request. In some aspects, a purpose of the authentication request may include the creation of a relationship (e.g., a financial relationship, such as a bank account, brokerage account, credit card account, and/or loan account) with a commercial institution associated with member system **103**, or the performance of a service by member system **103** (e.g., a financial server, such as performing transactions in a financial account associated with the user, cashing a check provided by the user, and/or selling a cashier's check to the user). As would be appreciated by one of skill in the art, the above exemplary authentication purposes are not intended to be limiting. In some aspects, a result of the authentication request may include whether the purpose of the authentication request was achieved. For example, when the purpose of the authentication request was creation of a relationship, the result of the authentication request may indicate whether the relationship was created. As another example, when the purpose of the authentication request was performance of a service, the result of the authentication request may indicate whether the service was performed. As would be appreciated by one of skill in the art, the above exemplary authentication results are not intended to be limiting. In some aspects, information related to the authentication request may include additional contact information, demographic information, financial information, or similar personal information provided in connection with the authentication request. In some aspects, such information may merely indicate that such information was provided, and/or provide a location where such information may be obtained. In some aspects, authentication record **307** may be obfuscated or encrypted according to methods known to one of skill in the art. For example, authentication record **307** may be encrypted with a cryptographic key.

(29) Cryptographic keys may be used to encrypt elements of messages in blocks, consistent with disclosed embodiments. In some aspects, such cryptographic keys may be associated with members of authentication system **100** (e.g., member system **103** or root system **107**). In various aspects, at least some of the cryptographic keys may be associated with authorized systems. Corresponding cryptographic keys may be available to decrypt the encrypted message elements, consistent with disclosed embodiments. For example, when an element of a message in a block is encrypted with a symmetric key, the same symmetric key may be available for decrypting the encrypted element. As another example, when an element of a message in a block is encrypted with a private key, a

corresponding public key may be available for decrypting the encrypted element. In some aspects, the corresponding cryptographic keys may be available to members of authentication system (e.g., member system **103** and root system **107**).

(30) FIG. **3**B depicts a logical model of identification data **309** stored in database **109**, consistent with disclosed embodiments. In some aspects, identification data **309** may comprise sensitive personal information, such as a social security number, taxpayer identification number, financial information, health information, employment information, demographic information, or other personal information disclosure of which might harm or embarrass the user. In various aspects, identification data **309** may comprise information gathered in compliance with statutory or regulatory guidelines for identifying customers, such as "Know Your Customer" guidelines under the USA Patriot Act. In some aspects, identification data **309** may comprise an indication of a method used to authenticate a user to the commercial institution associated with root system **107**. For example, identification data **309** may indicate that a driver's license with a particular driver's license number was presented to representatives of the commercial institution. As an additional example, identification data **309** may comprise an image of the driver's license.

(31) In some embodiments, identification data **309** may be encrypted according to methods known to one of skill in the art. For example, identification data **309** may be encrypted using the Advanced Encryption Standard (AES) or similar encryption methods. As would be appreciated by one of skill in the art, a cryptographic key may be used to decrypt identification data **309**. For example, root system **107** may be configured to generate a root system key for encrypting entries stored in database **109** by root system **107**. Root system **107** may be configured to provide the root system key to other members of authentication system **100**. In some embodiments, identification data **309** may be combined with a cryptographic salt prior to encryption. In some embodiments, the cryptographic salt may be a value specific to root system **107**. Converting identification data **309** to plaintext may require knowledge of the cryptographic salt, as would be understood by one of skill in the art. In some aspects, root system **107** may be configured to provide the cryptographic salt to other members of authentication system **100**. In some embodiments, identification data **309** may be combined with a cryptographic pepper prior to encryption. In some embodiments, the cryptographic pepper may be common to all entries in database **109**. Converting identification data **309** to plaintext may require knowledge of the cryptographic pepper, as would be understood by one of skill in the art.

(32) FIG. **4** depicts an exemplary process for establishing a user identity in the context of authentication system **100**, consistent with disclosed embodiments. In some embodiments, root system **107** may be configured to establish a user identity in step **401**. For example, root system **107** may be configured to receive personal information for the user. As depicted in FIG. **4**, root system **107** may be configured to receive at least some of the personal information from the user. Root system **107** may be configured to receive this information directly from the user. For example, the user may interact with an input/output interface of root system **107**. Root system **107** may be configured to receive this information indirectly from the user. For example, root system **107** may be configured to receive the personal information from an agent or constituent of the user, or from an operator of the authentication system (e.g., an employee of a commercial institution associated with root system **107**). Root system **107** may be configured to receive this information from a system associate with the user, such as user system **101**. The content of the personal information may depend on statutory or regulatory guidelines for identifying customers, such as "Know Your Customer" guidelines under the USA Patriot Act. The receipt of the personal information may satisfy these guidelines. In some aspects, root system **107** may be configured to augment the personal information with information retrieved from other sources, such as information retrieved from public records, credit reporting agencies, or other sources.

(33) In some embodiments, prior to establishing a user identity, member system **103** may be configured to determine that authentication system **100** lacks an identity for the user. For example,

member system **103** may be configured to determine that blockchain **105** does not include a block corresponding to the user. This determination may use the personal information provided by the user, the index information stored in blockchain **105**. For example, member system **103** may be configured to use probabilistic matching methods known to one of skill in the art, as describe below with respect to step **503**, to determine that blockchain **105** does not include a block corresponding to the user.

(34) Root system **107** may be configured to store a message to blockchain **105** in step **403**, consistent with disclosed embodiments. In some aspects, the message may comprise index information **303** and root system information **305**. Root system **107** may be configured to generate index information **303** using the personal information. For example, root system **107** may be configured to generate a hash of a portion of the personal information. As an additional example, root system **107** may be configured to encrypt a portion of the personal information. As noted above, this personal information may be received directly or indirectly from the user, and may be augmented with information received from other sources. Root system **107** may be configured to generate root system information **305** using configuration information for root system **107**. In some aspects, this configuration information may be predetermined. In various aspects, this information may be dynamically discovered by root system **107**, according to methods known to one of skill in the art. In some aspects, root system **107** may be configured to add blocks containing the messages to blockchain **105**. In various aspects, root system **107** may be configured to provide the messages to an authorized system. The authorized system may be configured to add blocks containing the messages to blockchain **105**.

(35) Root system **107** may be configured to store identification data **309** to database **109** in step **405**, consistent with disclosed embodiments. Root system **107** may be configured to generate identification data **309** using the personal information. As noted above, this personal information may be received directly or indirectly from the user, and may be augmented with information received from other sources. As described above, identification data **309** may be encrypted using the Advanced Encryption Standard (AES) or similar encryption methods. In some aspects, root system **107** may be configured to encrypt identification data **309** prior to storage in database **109**. In various aspects, database **109** may be configured to encrypt identification data **309** upon receipt of identification data **309** from root system **107**.

(36) FIG. **5** depicts an exemplary process for authenticating a user, consistent with disclosed embodiments. In some aspects, member system **103** may be configured to receive an authentication request in step **501**. Member system **103** may be configured to receive the authentication request directly from the user. For example, the user may interact with an input/output interface of member system **103**. Member system **103** may be configured to receive this information indirectly from the user. For example, member system **103** may be configured to receive the personal information from an agent or constituent of the user, or from an operator of the authentication system (e.g., an employee of the commercial institution associated with member system **103**).

(37) Member system **103** may be configured to determine root system **107** using blockchain **105** in step **503**, consistent with disclosed embodiments. In some aspects, member system **103** may be configured to read blockchain **105** to determine whether at least one entry exists for the user. As a non-limiting example, member system **103** may be configured to receive personal information, such as a first name, last name, and date of birth from the user. Member system **103** may be configured to compare this information to index information **303** retrieved from blocks in blockchain **105**. For example, member system **103** may be configured to determine index information **303** most likely corresponding to the user. In some aspects, member system **103** may be configured to determine index information **303** most likely corresponding to the user according to methods known to one of skill in the art. In some aspects, member system **103** may be configured to convert index information **303** to plaintext as part of this comparison. In various aspects, member system **103** may be configured to compares a hash stored in index information

303 to a hash generated using the received personal information.

(38) Root system **107** may be configured to authenticate the user in step **505**, consistent with disclosed embodiments. In some embodiments, member system **103** may be configured to direct the user to root system **107** for authentication. For example, member system **103** may be configured to provide a redirection message to user system **101**, or another system associated with the user, according to methods known to one of skill in the art. In some aspects, this redirection message may include an identifier for an Open ID endpoint associated with root system **107**, as described in OpenID and incorporated herein by reference. Root system **107** may be configured to receive credentials from the user system **101**, or another system associated with the user. For example, root system **107** may be configured to receive a username and password. Root system **107** may be configured to authenticate the credentials according to methods known to one of skill in the art. In some embodiments, root system **107** may be configured to perform multi-factor authentication of the user. In some aspects, root system **107** may be configured to provide a consent message including a confirmation code to another device associated with the user. Root system **107** may be configured to provide the consent message after successfully authenticating the credentials. As non-limiting examples, root system **107** may be configured to send a text message including the confirmation code to a predetermined number of the user, or an email including the confirmation code to a predetermined email address of the user. Root system **107** may be configured to receive from user system **101**, in response to the confirmation message, the confirmation code.

(39) Member system **103** may be configured to receive a root system secret in step **507**, consistent with disclosed embodiments. In some aspects, root system **107** may be configured to provide a verification message to member system **103**. For example, root system **107** may be configured to provide the verification message upon successful completion of multi-factor authentication in step **505**. In some aspects, the verification message may indicate successful completion of the multi-factor authentication. The verification message may include an authorization code. The authorization code may enable member system **103** to retrieve the root system secret from root system **107**.

(40) In some aspects, root system **107** may be configured to provide an authorization token to member system **103**. The authorization token may comprise a OAuth authorization security token, as described in “The OAuth 2.0 Authorization Framework,” by the Internet Engineering Task Force, incorporated herein by reference in its entirety Root system **107** may be configured to delegate authorization to member system **103** to access database **109** by providing the authorization token to member system **103**. In further aspects, root system **107** may be configured to provide at least one of the root system key and cryptographic salt, described above with regards to FIG. **3**B, to member system **103**. In some embodiments, root system **107** may be configured to provide at least one of the authorization token, the root system key, and the cryptographic salt in response to receiving the authorization code from member system **103**.

(41) Member system **103** may be configured to receive identification data **309** in step **509**, consistent with disclosed embodiments. In some embodiments, database **109** may be configured to provide identification data **309** in response to receiving the authorization token from member system **103**. In some aspects, database **109** may be configured to provide encrypted identification data **309** to member system **103**. Member system **103** may be configured to use at least one of the root system key and the cryptographic salt to decrypt identification data **309**. In some aspects, member system **103** may be configured to provide at least one of the root system key and the cryptographic salt to database **109**. In response, database **109** may be configured to decrypt identification data **309**, and to provide the decrypted identification data **309** to member system **103**.

(42) Member system **103** may be configured to receive complete authentication of the user in step **511**, consistent with disclosed embodiments. In some embodiments, member system **103** may be configured to use the decrypted identification data **309** to complete authentication of the user. For example, when the user requests authentication in the context of a business process subject to

statutory or regulatory requirements, such as “Know Your Customer” requirements, the decrypted identification data **309** may be sufficient to satisfy these requirements. In some embodiments, the decrypted identification data **309** may be provided to the user. For example, member system **103** may be configured to provide the decrypted identification data **309** to user system **101**. In some embodiments, member system **103** may be configured to pre-populate a form with the decrypted identification data **309**, and provide this prepopulated form to the user. User system **101**, or another system, may be configured to receive additional information from the user, and update the prepopulated form with this information. User system **101**, or another system, may be configured to provide this update form to member system **103**.

(43) Member system **103** may be configured to store authentication information for the authentication request in step **513**, consistent with disclosed embodiments. The authentication information may comprise index information **303**. The authentication information may comprise authentication record **307**. As described above with regards to FIG. **3**A, authentication record **307** may comprise information enabling subsequent auditing of transactions.

(44) FIG. **6** depicts exemplary user interfaces for multi-factor authentication, consistent with disclosed embodiments. In some embodiments, these user interfaces may be present on user system **101**, and on another device associated with the user (such as a computer, mobile phone, tablet, smartwatch, or similar device). Member system website **601** may comprise a website for member system **103**. In some aspects, member system website **601** may comprise an authentication page for member system **103**. For example, member system website **601** may comprise a login page, or a page for generating a new account with a commercial institution associated with member system **103**. As described above with regard to FIG. **5**, in response to an authentication request received from user system **101**, member system **103** may be configured to provide a redirect message to user system **101**. As shown in FIG. **6**, user system **101** may be configured to create another window containing login screen **603** in response to the redirect request. In some aspects, login screen **603** may enable the user to provide authentication credentials for root system **107**. For example, login screen **603** may be configured to allow the user to enter the authentication credentials into credentials control **605**. Credentials control **605** may comprise a text box, menu, radio button, or other control known to one of skill in the art.

(45) As described above with regard to FIG. **5**, in response to authentication of credentials provided by user system **101**, root system **107** may provide a consent message. This consent message may be provided to another device associated with the user. In some embodiments, this device may display application interface **611**. In some aspects, application interface **611** may include a message, describing the purpose and use of the consent message. Application interface **611** may comprise confirmation control **615**. In some aspects, application interface **611** may be configured to allow the user to select confirmation control **615** to complete multi-factor authentication with root system **107**. In various aspects, confirmation control **615** may display a code. The user may be required to entire this code into another user interface (e.g., login screen **603**) to complete multi-factor authentication with root system **107**.

(46) FIG. **7** depicts a schematic of exemplary computing system **700** for performing the envisioned systems and methods, consistent with disclosed embodiments. In some embodiments, computing system **700** includes a processor **710**, memory **715**, display **720**, I/O interface(s) **725**, and network adapter **730**. These units may communicate with each other via bus **735**, or wirelessly. The components shown in FIG. **7** may reside in a single device or multiple devices.

(47) Consistent with disclosed embodiments, processor **710** may comprise a central processing unit (CPU), graphical processing unit (GPU), or similar microprocessor having one or more processing cores. Computing system **700** may include one or more processors **710** and may further operate with one or more other processors that are remote with respect to processors **710**. Memory **715** may include non-transitory memory containing non-transitory instructions, such as a computer hard disk, random access memory (RAM), removable storage, or remote computer storage. In some

aspects, memory **715** may be configured to store data and instructions, such as software programs. For example, memory **715** may be configured to store data and instructions. In some aspects, processor **710** may be configured to execute non-transitory instructions and/or programs stored on memory **715** to configure computing system **700** to perform operations of the disclosed systems and methods. In various aspects, as would be recognized by one of skill in the art, processor **710** may be configured to execute non-transitory instructions and/or programs stored on a remote memory to perform operations of the disclosed systems and methods.

(48) Display **720** may be any device which provides a visual output, for example, a computer monitor, an LCD screen, etc. I/O interfaces **725** may include hardware and/or a combination of hardware and software for communicating information to computing system **700** from a user of computing system **700**, such as a keyboard, mouse, trackball, audio input device, touch screen, infrared input interface, or similar device. Network adapter **730** may include hardware and/or a combination of hardware and software for enabling computing system **700** to exchange information using external networks, such as network **111**. For example, network adapter **730** may include a wireless wide area network (WWAN) adapter, a Bluetooth module, a near field communication module, or a local area network (LAN) adapter.

(49) Other embodiments will be apparent to those skilled in the art from consideration of the specification and practice of the disclosed embodiments disclosed herein. It is intended that the specification and examples be considered as exemplary only, with a true scope and spirit of the disclosed embodiments being indicated by the following claims. Furthermore, although aspects of the disclosed embodiments are described as being associated with data stored in memory and other tangible computer-readable storage mediums, one skilled in the art will appreciate that these aspects can also be stored on and executed from many types of tangible computer-readable media, such as secondary storage devices, like hard disks, floppy disks, or CD-ROM, or other forms of RAM or ROM. Accordingly, the disclosed embodiments are not limited to the above described examples, but instead is defined by the appended claims in light of their full scope of equivalents.

(50) Moreover, while illustrative embodiments have been described herein, the scope includes any and all embodiments having equivalent elements, modifications, omissions, combinations (e.g., of aspects across various embodiments), adaptations or alterations based on the present disclosure. The elements in the claims are to be interpreted broadly based on the language employed in the claims and not limited to examples described in the present specification or during the prosecution of the application, which examples are to be construed as non-exclusive. Further, the steps of the disclosed methods can be modified in any manner, including by reordering steps or inserting or deleting steps. It is intended, therefore, that the specification and examples be considered as example only, with a true scope and spirit being indicated by the following claims and their full scope of equivalents.

APPENDIX A

(51) A. Exemplary Implementation

(52) Creates a blockchain utility tool that leverages (OpenID Connect) OIDC capabilities to control access and maintain security of access to data on a private distributed blockchain. Creates a blockchain utility tool that allows miners to look up encrypted identity attributes (email, fname, lname, phone number) on the private distributed blockchain to verify if the identity has already been verified via acceptable KYC methods. The utility tool upon successful match of said attributes will redirect the customer to the correct OIDC endpoint for the FI that added the verified identity to the blockchain. The customer will authenticate with the credentials for that FI to retrieve and OAuth token and the tokenized decryption key. With that key, the mining bank can retrieve the tokenized personal identifying information (PII) associated with the blockchain attributes (SSN, DOB, address, etc.) in order to populate the application form.

(53) B. Actors, Entities, Definitions

(54) 1. BlockChain Member: Financial Institutions (FIs) that are members of a private distributed

identity blockchain adhere to the agreed upon smart contract guidelines. 2. Customer: A prospective consumer that is applying for some product (Traditional FI, Identity only) with an FI on a private distributed identity blockchain. 3. BlockChain Miner: Associates of the FIs on the private distributed blockchain that continually mine the blockchain for updates to Identity data in order to validate that data 4. Root System: Provides identity and verification service with the power of multi-factor authentication.

C. Process Flow 1. A potential customer goes to entity A to apply online for a service. 2. Customer enters basic information on the application; email address, full name and phone number. 3. Entity A uses the blockchain utility too to call an API to lookup those attributes on the blockchain in real time. If the attributes are matched, proceed to step 7. 4. If the attributes are not a match, then Entity A presents BAU application flow for the customer to complete application and gather identity data to perform KYC. 5. Upon successful completion of KYC, Entity A updates the blockchain with encrypted email, full name and phone number so other FIs on the private blockchain can find it. 6. Entity A then adds all of the PII attributes to a distributed hashed table using agreed upon hash/salt protocols members of the BC agreed to. 7. Upon a successful match of the initial attributes, Entity A points the customer to the correct OIDC endpoint associated with Entity B, who is the FT that first added the verified identity to the blockchain. 8. The Customer is then prompted to authenticate with their credentials for Entity B. Upon a successful authentication, an OAuth token and a decryption key are provided back to Entity A. 9. Entity A then uses that key to call Entity B's distributed hash table via the external API gateway where the hashed PIT identity attributes are stored. 10. Entity A retrieves the PIT and populates their application form for the customer and completes the process w/o the need to conduct further KYC actions.

Claims

1. An authentication system comprising: one or more processors and non-transitory media storing instructions that, when executed by the one or more processors, cause operations comprising: receiving a request from a root system to publish a root system block to a private blockchain comprising blocks, the root system block being generated by the root system for a user and comprising root information identifying the root system and authentication data related to the user, the root system being distinct from the user and being a member system having access to the blockchain; publishing the root system block to the blockchain; subsequent to publishing the root system block to the blockchain, receiving an authentication request for the user; and based on the blockchain comprising at least one block for the user that includes the root information identifying the root system, providing the root information as part of a response to the authentication request.

2. The authentication system of claim 1, wherein the root system block comprises the root information identifying the root system and an authentication record for the user.

3. The authentication system of claim 2, wherein the authentication record for the user identifies at least one of the member system, an institution associated with the member system, or an authentication result.

4. The authentication system of claim 1, wherein the root system block comprises the root information identifying the root system and indexing information identifying the user.

5. The authentication system of claim 1, wherein the root information indicates a location of the root system or a location service for obtaining the location of the root system.

6. A method comprising: receiving a request from a root system to publish block data for a user to a private blockchain comprising blocks, the block data comprising root information identifying the root system and authentication data related to the user, the root system being distinct from the user and being a member system having access to the blockchain; publishing the block data to the blockchain; subsequent to publishing the block data to the blockchain, receiving an authentication request for the user; determining that the blockchain comprises at least one block for the user that

includes the root information identifying the root system; and based on the blockchain comprising the at least one block for the user that includes the root information identifying the root system, providing the root information as part of a response to the authentication request.

7. The method of claim 6, wherein the block data comprises the root information identifying the root system and an authentication record for the user.

8. The method of claim 7, wherein the authentication record for the user identifies at least one of the member system, an institution associated with the member system, or an authentication result.

9. The method of claim 7, wherein the block data comprises the root information identifying the root system and indexing information identifying the user.

10. The method of claim 7, wherein the root information indicates a location of the root system or a location service for obtaining the location of the root system.

11. The method of claim 7, wherein the blocks of the blockchain are added by miners via a consensus mechanism for the blockchain.

12. The method of claim 7, further comprising: based on the blockchain comprising the at least one block for the user that includes the root information identifying the root system, providing the root information and the authentication data related to the user as part of the response to the authentication request.

13. One or more non-transitory computer-readable media storing instructions that, when executed by one or more processors, cause operations comprising: receiving a request from a root system to publish block data for a user to a private blockchain comprising blocks, the block data comprising root information identifying the root system and authentication data related to the user, the root system being distinct from the user and being a member system having access to the blockchain; publishing the block data to the blockchain; subsequent to publishing the block data to the blockchain, receiving an authentication request for the user; based on the blockchain comprising at least one block for the user that includes the root information identifying the root system, providing the root information as part of a response to the authentication request.

14. The one or more non-transitory computer-readable media of claim 13, wherein the root system block comprises the root information identifying the root system and an authentication record for the user.

15. The one or more non-transitory computer-readable media of claim of claim 14, wherein the authentication record for the user identifies at least one of the member system, an institution associated with the member system, or an authentication result.

16. The one or more non-transitory computer-readable media of claim 13, wherein the root system block comprises the root information identifying the root system and indexing information identifying the user.

17. The one or more non-transitory computer-readable media of claim 13, wherein the root information indicates a location of the root system or a location service for obtaining the location of the root system.

18. The one or more non-transitory computer-readable media of claim 13, wherein the blocks of the blockchain are added by miners via a consensus mechanism for the blockchain.

19. The one or more non-transitory computer-readable media of claim 13, wherein the blocks of the blockchain are added via a proof-of-work condition for the blockchain.

20. The one or more non-transitory computer-readable media of claim 13, the operations further comprising: based on the blockchain comprising the at least one block for the user that includes the root information identifying the root system, providing the root information and the authentication data related to the user as part of the response to the authentication request.