

Identity on a Network**[0001] Technical Field**

[0002] The present invention relates to the field of distributed ledgers, and more specifically to the field of establishing and proving identity using a distributed ledger such as a blockchain.

[0003] Background

[0004] A useful application of distributed ledger systems such as blockchains is maintaining people's identities. Currently there are no widely used or scalable solutions for personal identity management that allow growth of identity information over time, identity information's use controlled by the identity holder, and trustless identity usage where no central authority oversees identity transactions. Many computing networks are overrun with bots or fraudulent accounts where the system is intended to be used by single users, but where the lack of an identity solution keeps these fraudulent activities from being prevented. Many systems that rely on identity, like voting, are cumbersome and rely on slow manual processes to try to avoid fraud, which creates inefficiencies. Many identity solutions and methodologies used now have problems with fraud. For example, a criminal who simply gets access to private information associated with identity, such as social security number, full name, address, phone number, etc. can use that information for identity theft. It can take years to fix problems associated with identity theft. Also, many identity solutions do not have sufficient controls on how identity information is used and lack a sufficient level of privacy. A blockchain identity solution can be used to alleviate or solve such problems.

[0005] Description of Invention

[0006] This application is related to US provisional applications 63123434 filed 12/9/2020, and 63123436 filed 12/9/2020. Each of the foregoing is incorporated herein by reference. The inventions described herein can be practiced in cooperation with the technology disclosed in PCT applications PCT/US2018/053240, PCT/US2018/053242, and PCT/US2018/053243, each filed 9/27/2018; and US application 16/808094, filed 3/123/2020; each of which is incorporated herein by reference.

[0007] Identity management in the present invention can include several operational steps such as identity verification by a third party, identity inquiries, and inquiry approval by the identity holder. A user's identity representation can comprise identity components. Identity components can refer to any aspect of a user's identity representation, such as name, age, social security number, passport number or scan, government id number, address, gender, nationality, facial recognition data, fingerprint data, genetic data, eye scan data, picture of the user, voice analysis data, body movement data, scans or pictures of documents the user owns such as passports or real-ID identification, scans or pictures of documents that prove aspects of a user's identity such as a utility bill with an address on it, medical history, dental records, blood type or other body characteristics, other biometric data, analysis on hair or cell samples, groups the user is involved with, other users the user is friends with, purchase history and spending patterns, internet usage data and patterns, user activities, or artificial intelligence or other

algorithmic analysis of any other data related to the user, as examples. Identity components such as these can be owned and controlled by the user in a blockchain wallet, in which tokens, json or binary wrappers, digital coins, or other representations of the identity component are associated with the user's wallet. For example a token can include an on-chain binary data string representing DNA information for the user, and that token can be held as an asset in the user's wallet where the user controls a private key associated with a public address, where the private key is used to add, modify, or use the identity information. Identity components can be held in a public address that is separate from other assets and transactions in order to keep identity information and maintenance separate from other types of transactions.

[0008] Identity components can be verified by third parties as part of the identity representation. For example, a business in a physical location can provide identity verification services, where a user can present a real-ID identification, for example, and that business can send a token to the user's public address on a blockchain with verification information in a token representing the real-ID identification. Identity verifiers can sign tokens or use other cryptographic techniques to prove their validity. Identity verifiers can record identity verification information so that identity can be re-sent to a holder's wallet at a later time, such as for account recovery. For example, if a user's private key is compromised, the user's identity information might need to be recreated in a new wallet. An identity verifier can take a picture of the user along with a scan of a real-ID, both of which can be stored, so that the identity information can be recovered in the future without the need for another in person visit. Data can be encrypted using the user's public key or other types of encryption methods, so that others who can see the blockchain cannot understand or decipher the information contained in the token and on the blockchain.

[0009] The verifying company can refuse to create the token if the picture on a physical identification does not look like the person getting the verification, for example, and trust in that component can represent trust in the verifying entity doing its job properly. The collection of a variety of identity components can create a higher probability of a correct identity verification. Where a single component might be flawed in some way, multiple components that are validated by different identity verifiers are likely to be more accurate in correctly identifying a person, when taken as a whole.

[0010] There are many ways that identity components can be verified. Examples include, without limitation, an identity verifier who collects and stores pictures of users holding their passport where their face and the passport information can be clearly seen; an identity verifier that collects and stores multiple sources of data at once, whether in person or transmitted electronically, as an example including a collection of data such as a birth certificate, photo ID, passport, proof of address, and bio-signature; a DNA company that places encrypted DNA information on-chain; a phone application that takes a fingerprint scan and a retina scan; a government authority allowing people to enter a country upon taking a face scan; a dentist or doctor or medical facility adding information related to a person's health; an online site adding information related to purchasing information; a credit company maintaining a

blockchain representation of credit; a drug testing facility adding test results; a voting center adding voter registration information to a user's wallet after collecting physical identity information; and a voting center adding voter registration information to a user's wallet after verifying blockchain identity information. Identity verifiers, for example, can also require identity inquiries be successfully passed on existing identity components in a wallet before new identity information can be added.

[0011] Identity verifiers can be permissioned by a controlling entity on the system so that all of their verifications can be revoked if they provide fraudulent or careless identity verifications. For example, if a company is permissioned to provide verified identification tokens, and it is later found out that the company provided those identification tokens fraudulently, then all identities provided by that identity verifier can be removed from the blockchain. Tokens can be destroyed, transferred, invalidated or otherwise set so that they can no longer be used. In the case that identity components that are removed are correlated with other identity components, those correlations can be removed or invalidated as well.

[0012] Identity components can be correlated or connected. Correlations between identity components can be maintained on an immutable representation of identity, such as a representation commonly held on a blockchain, so that the record of those correlations are assured to not change, even if the correlations need to be updated or modified. Correlations can represent more than the simple fact that identity components are located in the same wallet. An example of a correlation is an identity verifier who verifies multiple identity components at once, and where the identity components are added to a user's wallet at the same time. In this example, the identity verifier can evaluate a birth certificate, then evaluate a real-ID picture ID in an in-person setting where the ID can be compared to the person's face, then evaluate a current utility bill that includes an address and a date.

[0013] When the identity verifier adds each of those components into the user's wallet, they can be recorded in a way that their correlations are described on-chain. A birth certificate identity component can be added with information from the birth certificate, a real-ID component can be added with information from the real-ID, a scan of the utility bill can be added to a utility bill identity component, an address identity component can be added, a payment indicator component can be added, and correlations between all of these components can be added. In this example, a variety of correlations can be included in the identity representation. For example, because the user was in physical possession of the documents when the identity information was taken, that fact can be individually added to each identity component. Each component can include information that it was input at the same time as the other components, and that information across components was verified at that time. Someone later needing a query to the birth certificate component, for example, would be able to validate that it was verified in person alongside a real-ID with a photo that was compared to the person providing the information. All of the components can be described on-chain that they were verified at the same time. Where a utility bill might be easy to fraudulently forge, a passport is more difficult to forge, so the fact that it is taken by the same identity verifier and that the information on both documents was

corroborated against each other, makes it less likely that the utility bill was forged. A sole birth certificate identity component on its own is statistically less likely to represent a valid ID than a birth certificate that was verified at the same time as a picture id. Recording correlations makes fraud in an overall identity representation more difficult.

[0014] There are a variety of ways that correlations can be described in software, known to those skilled in the art. For example, identity tokens can include a Json representation in which that representation includes an array of other identity components that are correlated, how they are correlated, the date the correlations are made, and the verifying authority that made the correlation, as an example. The description of how they are correlated can include concepts such as components that are verified against each other, taken at the same time, owned or controlled by the same person, linked through other identity components, linked against biometric data, linked through analysis or artificial intelligence algorithms, or any other way that two or more identity components can be shown to have some type of correlation. For example, identity components can be correlated to a biometric signature such as a retinal scan, which is difficult to forge.

[0015] As an example embodiment of the present invention, an identity verifier can require that all identity components that it issues to a wallet be correlated against a retinal scan where the retinal scan is compared to on-chain retinal scan data in the wallet. As another example, an identity verifier can require that all identity components be correlated against a DNA sample where that sample is compared against an on-chain representation of DNA before the new component is added.

[0016] Correlations can be directly recorded or can be inferred. For example, correlations can be added through algorithms or artificial intelligence. A user who purchases items on an online site inherently produces buying patterns. Analysis of those buying patterns can be automatically added to existing components or to a special purpose component intended specifically to show buying patterns. A buying pattern component, for example, can be used to prevent unusual purchases that do not fit previous buying patterns without additional identity verification.

[0017] Correlations can be added over time. A correlation that did not exist at the time the identity component was created can be added later as new information becomes available. For example a real-ID component can be added, then a month later a birth certificate can be taken to a verifier with the real-ID in hand, and the real-ID component can be updated to be correlated with the birth certificate. These types of additions can be done on an immutable chain so the time ordered progression of correlations is recorded. The time ordered progression of correlations itself can be used to further strengthen an identity verification. For example, patterns of identity component additions or modifications, as well as a longer term history of identity component validations can indicate a non-compromised account. Correlations can also occur through identity components. For example, a birth certificate that is correlated to an in person viewing by an identity verifier alongside a real-ID picture id can be directly correlated to an address component later verified alongside the same real-ID picture. Therefore in this

example, an inquiry that inquires about a birth certificate associated with that address can state in the inquiry that that type of indirect correlation satisfies the inquiry criteria, and the identity inquiry associating the birth certificate with an address can pass.

[0018] Correlations can be time limited. For example, a correlation between a real-ID component and an address component can be set to only be valid for three months. Similarly components themselves can be set to only be valid over a set timeframe. An identity verifier can record that the verification on a passport is only valid through the expiration date of the passport, or as another example, it can only be valid for a shorter time period, so that a face comparison against the picture in the passport needs to be verified on a shorter timeframe.

[0019] After identity components are added to a wallet or other ownership representation on a distributed ledger, that overall identity profile can be queried against. There are a variety of uses for identity information and identity profiles maintained in the present invention. Examples of uses for identity in the present invention include, without limitation, a voting system that requires proof that an individual has a right to vote; a payment system that requires proof of identity for making a purchase; a home lender approving a mortgage; a dating site that requires verification of identity information for use on the site such as age or gender; a credit card company issuing a new credit card; a bank opening a new bank account; two individuals making a transaction between each other; insurance claims; a government verifying who can enter a country or not; a building verifying who can enter; systems that allows users to rent a car, rent a bike, rent a scooter, or use a service such as a car ride or food delivery; stores selling alcohol or other age-limited items; online services, sites, applications, or games that have requirements such as age restrictions or nationalities; a social media network where proof of expertise or other characteristics are used to convey information; social media information that influences elections; site and information dissemination where bots are not wanted; paying taxes and receiving tax refunds; control of identity usage where the control of the information is more important than the information itself, such as when looking to prevent identity theft; or financial transaction systems. In these examples an entity can inquire against the identity profile comprised of the identity components.

[0020] Identity inquiries can include an inquiry for the existence of an identity component. For example, an inquiry can inquire if a validated real-ID component exists in a wallet, if a passport component exists in a wallet, or if any address component exists in a wallet. Identity inquiries can include inquiries about the state of a component. For example, an inquiry can inquire if an address component was verified in the past 30 days, if a passport has expired, if a component has specific correlations to other components, if a component has been modified, or who a component was last verified by.

[0021] Inquiries of an identity profile can be based largely or wholly on correlations. For example an inquiry on a person's identity by a lender can require that an identity verifier verified multiple specific identity components at the same time, that a picture ID was included in that set and that the picture ID is shown to have been compared with the person's face in-person. As another example, an inquiry into a

user's ID can require that each of 5 separate and specific identity components exists and that each are correlated with a retinal scan included in the user's wallet.

[0022] Both the existence of identity components as well as correlations between identity components can be used to prevent fake or fraudulent identity accounts as well as duplicated identity accounts. For example, before a real-ID identity verification is added to a wallet, the identity verifier can inquire against all identity blockchain records that that real-ID license number does not already exist in any other wallet. Similarly, the blockchain system itself can be defined so that it is impossible for duplicate fields on specific identity components to be repeated. For example, the consensus mechanism for the blockchain can prevent two wallets from both containing a passport identity component with the same country and passport number. Before a social security identity component is added, a check can be made that no other social security component exists in any other wallet with the same social security number.

[0023] Correlations can be used to detect and prevent multiple wallets used by the same individual or fraudulent identity accounts. For example, a correlation between an address component and other components can be compared against address components in other wallets. Where two people who live in the same house might have the same address in an address component, correlations can show that a single person has multiple identity accounts. If a user has multiple identity accounts, the accounts can be required to be merged. Similarly, DNA can be correlated with full formal names. Formal names can be further verified and correlated against other identity components. Where an accurate DNA comparison across all DNA identity components for all users might not be feasible in terms of computational processing power, a subset of DNA checks can be performed against user's last names, for example, making the comparisons of DNA information more practical. In that example, a user can quickly recover a compromised account based on their name and DNA information.

[0024] If a criminal who wants to steal someone's identity were to try and duplicate other identity components of the victim, that identity theft would be made much more difficult if DNA is included in the verification of identity components, where the DNA identity component is correlated with other identity components that are added to the victim's wallet at the same time the DNA identity component is added. In that situation, an identity thief might be able to later forge some documents, but it would be difficult to forge DNA results. The victim of an identity theft attempt would be able to show that other identity components the thief added to a fraudulent wallet are indeed fraudulent, which would clear up the victim's use of their identity profile.

[0025] If a user's private key or other method of maintaining sole access to identity is compromised, for example if a private key is stolen, that user can work with identity verifiers to revoke identity components added into the compromised wallet or account. Correlations can play an important role in defining and recovering a compromised account. An identity component that is revoked by an identity verifier can be used to automatically revoke any correlated identity components. For example, if all identity components in an account are correlated to a retina scan, and the owner discovers that an identity thief stole their

private key, then the user can describe to an identity verifier that their private key was stolen and take a retina scan with an identity verifier so that the identity verifier can then revoke the retina scan on the account therefore revoking all of the other identity components. The user can then create a new account or wallet, and add identity components back into it through identity verifiers.

[0026] If a user wants to remove personal information in the present invention, identity components can be removed or destroyed. For example, a user can send an identity component to an address that indicates that it should be destroyed. Additional methods of indicating a record should be deleted can be used including, without limitation, a transaction that defines the record should be deleted or an off-chain message to an authority, as examples. When validators or consensus providers in the system receive a valid transaction to a deletion address, for example, they can remove the data from the blockchain representation. This can be done in a way, for example, that the original merkle tree and the hashes that define the merkle tree are maintained to keep the blockchain intact, but the data that defined the hashes in the merkle tree, particularly in leaf nodes, is deleted from all consensus providers on the network. Shards or other types of partition in how a blockchain is processed can include special rules that are different than other shards. For example, an identity shard can be defined in a way that data can be removed from the blockchain where other shards can be defined in a way that no data can be altered on their blockchains.

[0027] Similarly, a user can protect private data by simply encrypting all identity information and protecting the private key. If a private key is stolen, that event can trigger the previously described methods of removing private information on the blockchain. Similarly, transactions involving private information can also be removed from a blockchain's records by the consensus providers. Similar to removing an identity component or identity information, details of identity related transactions can be removed from a blockchain by removing specific data while leaving hashes in relevant merkle trees. Additionally, privacy can be protected in the present invention by providing for a system that makes inquiries on identity information such that the inquiries are maintained off chain. For example, identity components can be recorded and maintained on-chain, but an inquiry on that data can be made through an encrypted off-chain message in which the results can be verified by the on-chain data.

[0028] Identity inquiries can be recorded on-chain, so that the inquiry and its results are specified by multiple consensus providers using information on-chain. By doing so, a record of identity inquiries and their results can be recorded and audited. This functionality can be used in a voting system, for example, where the voting authority desires to provide proof of the validity of an election. The results of any given vote associated with any given identity can be restricted from public disclosure, but proof that no individual voted more than once can be shown.

[0029] Identity inquiries can be processed off-chain. For example, a bank that needs to verify a user's identity can send a request to the user. The user can receive the request through an application, for example, and then respond to the request utilizing a private key that is used for protecting the user's

identity. Identity inquiries can include identity information as part of the request, so that the information needs to match in order to fulfill a request. For example, a user purchasing alcohol can take a fingerprint scan at the point of sale, and the request for verification that the user is over 21 can be required to match with both an identity component showing the user is over 21 as well as a fingerprint identity component that matches with the fingerprint scan taken at the time of purchase.

[0030] Once a user receives an identity verification request, the user can approve that identity verification request or not. The user can, for example, receive a request in an app that requests verification of age. The user can then send the recipient an age identity token verifying age, for example. Identity requests and identity request approval can happen on-chain or off-chain. An example, without limitation, of one type of an identity verification approval in a specific example situation is as follows. In this example, a voting location can require that a voter have a verified address, a verified name, a verified picture, a verified social security number, and verified biometric indicator such as a fingerprint scan. The user who is voting can have a wallet on a blockchain that includes those verified identity components. Those identity components can be encrypted on-chain and can previously have been verified by a third party. The user can use an application on their phone that includes the private key associated with the public address in the wallet holding the identity components. When the user arrives to the voting center, they can take a fingerprint scan. Data from the fingerprint scan can be used to create an inquiry for the user, which can appear, for example, as a QR code on a screen. The QR code can include transfer information as well, describing where the results of the request should be sent.

[0031] The user can scan the QR code on the voting screen with their app. The app can then indicate to the user the request for an approval to send the information to the voting station. The user can approve or deny the request, and since the user wants to vote, the user can approve the request in the app. The app then can use the private key held on the phone to send tokens verifying identity information to the voting station's wallet address, or it can also decrypt identity information to send to the recipient voting station. A secure connection can be created for transmitting any off-chain information through standard traditional processes for transmitting secure electronic data. The app can send data to the voting station or to a wallet associated with the voting station using signing techniques or other standard cryptographic techniques. For example, the picture information can be decrypted using the user's private key, then sent through a secure connection to the voting station where a person working at the voting station can see the picture and compare it to the user. Software running on a computer at the voting station can encrypt the picture with the user's public key to verify that it matches with the encrypted data on-chain, in order to verify authenticity. The voting station can also detect that other validly signed tokens, which can include signature proof from third party verifiers on the identity tokens, have been received in a wallet address associated with the voting station. In the same way that picture information was verified at the voting station location, on-chain fingerprint information can be verified against fingerprint information taken at the time by first decrypting it using the user's private key. Requests can also include biometric

data or other identifying information, and tokens can be transferred only if the request biometric data or other identifying information matches on-chain data.

[0032] Encrypted identity information can be held in a user's wallet to help provide security and privacy. Because identity information is encrypted, in many situations it does not need to be removed from the blockchain, where unencrypted data, in contrast, often needs to be removed from an online database. Similarly, data can be referenced with hashes, and then held in an off-chain database. Finally, the data held in a block's merkle tree can be culled by all validators so that the data itself is removed, but the hashes that comprise the merkle tree remain intact, which maintains the blockchain's integrity while removing personal information held on-chain.

[0033] Coins or tokens or any other form of on-chain representation of identity can be transferred from a user to a recipient through the blockchain's consensus mechanisms in order to validate identity for a request. Identity tokens can be held in a user's wallet, where the tokens' functionality can be defined through smart contracts. For example, a token verifying a user's age is over 21 can be held in the user's wallet, and the token can be defined in the blockchain system to be able to send copies to recipients as the user requests. In this way, tokens can be verified by third party verifiers, and the verified tokens can then be used to verify identity as many times as the token allows and in any conditions that the token allows. Tokens can, for example, be defined in a way that limits the number of times they can be used over a timeframe, the types of recipients that can receive an identity token, or any other limitation that can be implemented with a smart contract.

[0034] Approvals for identity requests can require additional information from the approver, beyond simply having access to the private key associated with a public address. For example, an identity approval, in order to be considered valid by consensus providers or validators or oracles, can require a separate password, a bio-signature, or two-factor authentication, as examples.

[0035] Identity components and correlations can represent functionality capabilities in smart contracts, such as the ability to use a credit card, transfer assets, or create transactions. Identity components and correlations can be required to take part in a system's use. This can, for example, be a useful tool in the removal of bots.

[0036] Identity components can be used to implement verification tiers. For example, a Tier 4 identity verification in a system can give a user rights that a lower tier identity verification level does not enable. The tiers can be defined by required components and required correlations that indicate an identity has been more thoroughly verified.

[0037] Identity request allowances, verifications, components, and correlations can be controlled by multiple wallets with varying permission levels. For example, tokens in a wallet can be defined such that they can be sent by the wallet's holder or by another wallet's holder. Permissions can vary for a containing-wallet holder or an associated-wallet holder. This can be used by a parent, for example, such

that the parent's permission is needed to allow information to be sent in response to an inquiry. Similarly, employers can have permissions for verifying identity based on its employees' identity components.

[0038] In this description, the term blockchain can refer to any distributed ledger, including distributed ledgers that are not literally blockchains. Wallets, accounts, and public addresses all refer to a representation of ownership of tokens or other assets and are not intended to be limiting in their descriptions.

[0039] **Implementation.** Methods and apparatuses according to the present invention can be implemented using multiple computers connected in a distributed network. Traditionally, a computer program consists of a finite sequence of computational instructions or program instructions. It will be appreciated that a programmable apparatus (i.e., computing device) can receive such a computer program and, by processing the computational instructions thereof, produce a further technical effect.

[0040] A programmable apparatus includes one or more microprocessors, microcontrollers, embedded microcontrollers, programmable digital signal processors, programmable devices, programmable gate arrays, programmable array logic, memory devices, application specific integrated circuits, or the like, which can be suitably employed or configured to process computer program instructions, execute computer logic, store computer data, and so on. Throughout this disclosure and elsewhere a computer can include any and all suitable combinations of a special-purpose computer, programmable data processing apparatus, processor, processor architecture, and so on.

[0041] It will be understood that a computer can include a computer-readable storage medium and that this medium can be internal or external, removable and replaceable, or fixed. It will also be understood that a computer can include a Basic Input/Output System (BIOS), firmware, an operating system, a database, or the like that can include, interface with, or support the software and hardware described herein.

[0042] Embodiments of the systems as described herein are not limited to applications involving conventional computer programs or programmable apparatuses that run them. It is contemplated, for example, that embodiments of the invention as claimed herein could include an optical computer, quantum computer, analog computer, or the like.

[0043] Regardless of the type of computer program or computer involved, a computer program can be loaded onto a computer to produce a particular machine that can perform any and all of the depicted functions. This particular machine provides a means for carrying out any and all of the depicted functions.

[0044] Any combination of one or more computer readable medium(s) can be utilized. The computer readable medium can be a computer readable signal medium or a computer readable storage medium. A computer readable storage medium can be, for example, but not limited to, an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system, apparatus, or device, or any suitable combination of the foregoing. More specific examples (a non-exhaustive list) of the computer readable storage medium include the following: an electrical connection having one or more wires, a portable

computer diskette, a hard disk, a random access memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory (EPROM or Flash memory), an optical fiber, a portable compact disc read-only memory (CD-ROM), an optical storage device, a magnetic storage device, or any suitable combination of the foregoing. In the context of this document, a computer readable storage medium can be any tangible medium that can contain, or store a program for use by or in connection with an instruction execution system, apparatus, or device.

[0045] According to an embodiment of the present invention, a data store can be comprised of one or more of a database, file storage system, relational data storage system or any other data system or structure configured to store data, preferably in a relational manner. In an embodiment of the present invention, the data store can be a relational database, working in conjunction with a relational database management system (RDBMS) for receiving, processing and storing data. In an embodiment, the data store can comprise one or more databases for storing information related to the processing of moving information and estimate information as well one or more databases configured for storage and retrieval of moving information and estimate information.

[0046] Computer program instructions can be stored in a computer-readable memory capable of directing a computer or other programmable data processing apparatus to function in a particular manner. The instructions stored in the computer-readable memory constitute an article of manufacture including computer-readable instructions for implementing any and all of the depicted functions.

[0047] A computer readable signal medium can include a propagated data signal with computer readable program code embodied therein, for example, in baseband or as part of a carrier wave. Such a propagated signal can take any of a variety of forms, including, but not limited to, electro-magnetic, optical, or any suitable combination thereof. A computer readable signal medium can be any computer readable medium that is not a computer readable storage medium and that can communicate, propagate, or transport a program for use by or in connection with an instruction execution system, apparatus, or device.

[0048] Program code embodied on a computer readable medium can be transmitted using any appropriate medium, including but not limited to wireless, wireline, optical fiber cable, RF, etc., or any suitable combination of the foregoing.

[0049] The elements depicted in any flowchart illustrations and block diagrams in the figures imply logical boundaries between the elements. However, according to software or hardware engineering practices, the depicted elements and the functions thereof can be implemented as parts of a monolithic software structure, as standalone software modules, or as modules that employ external routines, code, services, and so forth, or any combination of these. All such implementations are within the scope of the present disclosure.

[0050] In view of the foregoing, it will now be appreciated that elements of any block diagrams and flowchart illustrations support combinations of means for performing the specified functions,

combinations of steps for performing the specified functions, program instruction means for performing the specified functions, and so on.

[0051] It will be appreciated that computer program instructions can include computer executable code. A variety of languages for expressing computer program instructions are possible, including without limitation C, C++, Java, JavaScript, assembly language, Lisp, HTML, Perl, and so on. Such languages can include assembly languages, hardware description languages, database programming languages, functional programming languages, imperative programming languages, and so on. In some embodiments, computer program instructions can be stored, compiled, or interpreted to run on a computer, a programmable data processing apparatus, a heterogeneous combination of processors or processor architectures, and so on. Without limitation, embodiments of the system as described herein can take the form of web-based computer software, which includes client/server software, software-as-a-service, peer-to-peer software, or the like.

[0052] In some embodiments, a computer enables execution of computer program instructions including multiple programs or threads. The multiple programs or threads can be processed more or less simultaneously to enhance utilization of the processor and to facilitate substantially simultaneous functions. By way of implementation, any and all methods, program codes, program instructions, and the like described herein can be implemented in one or more thread. The thread can spawn other threads, which can themselves have assigned priorities associated with them. In some embodiments, a computer can process these threads based on priority or any other order based on instructions provided in the program code.

[0053] Unless explicitly stated or otherwise clear from the context, the verbs "execute" and "process" are used interchangeably to indicate execute, process, interpret, compile, assemble, link, load, any and all combinations of the foregoing, or the like. Therefore, embodiments that execute or process computer program instructions, computer-executable code, or the like can suitably act upon the instructions or code in any and all of the ways just described.

[0054] The functions and operations presented herein are not inherently related to any particular computer or other apparatus. It is possible to modify or customize general-purpose systems to be used with programs in accordance with the teachings herein, or it might prove convenient to construct more specialized apparatus to perform the required method steps. The required structure for a variety of these systems will be apparent to those of skill in the art, along with equivalent variations. In addition, embodiments of the invention are not described with reference to any particular programming language. It is appreciated that a variety of programming languages can be used to implement the present teachings as described herein, and any references to specific languages are provided for disclosure of enablement and best mode of embodiments of the invention. Embodiments of the invention are well suited to a wide variety of computer network systems over numerous topologies. Within this field, the configuration and management of large networks include storage devices and computers that are

communicatively coupled to dissimilar computers and storage devices over a network, such as the Internet.

[0055] Throughout this disclosure and elsewhere, block diagrams and flowchart illustrations depict methods, apparatuses (i.e., systems), and computer program products. Each element of the block diagrams and flowchart illustrations, as well as each respective combination of elements in the block diagrams and flowchart illustrations, illustrates a function of the methods, apparatuses, and computer program products. Any and all such functions ("depicted functions") can be implemented by computer program instructions; by special-purpose, hardware-based computer systems; by combinations of special purpose hardware and computer instructions; by combinations of general purpose hardware specialized through computer instructions; and so on - any and all of which can be generally referred to herein as a "circuit," "module," or "system."

[0056] While the foregoing drawings and description set forth functional aspects of the disclosed systems, no particular arrangement of software for implementing these functional aspects should be inferred from these descriptions unless explicitly stated or otherwise clear from the context.

[0057] Each element in flowchart illustrations can depict a step, or group of steps, of a computer-implemented method. Further, each step can contain one or more sub-steps. For the purpose of illustration, these steps (as well as any and all other steps identified and described above) are presented in order. It will be understood that an embodiment can contain an alternate order of the steps adapted to a particular application of a technique disclosed herein. All such variations and modifications are intended to fall within the scope of this disclosure. The depiction and description of steps in any particular order is not intended to exclude embodiments having the steps in a different order, unless required by a particular application, explicitly stated, or otherwise clear from the context.

[0058] The functions, systems and methods herein described can be utilized and presented in a multitude of languages. Individual systems can be presented in one or more languages and the language can be changed with ease at any point in the process or methods described above. One of ordinary skill in the art would appreciate that there are numerous languages the system could be provided in, and embodiments of the present invention are contemplated for use with any language.

[0059] While multiple embodiments are disclosed, still other embodiments of the present invention will become apparent to those skilled in the art from this detailed description. The invention is capable of myriad modifications in various obvious aspects, all without departing from the spirit and scope of the present invention. Accordingly, the drawings and descriptions are to be regarded as illustrative in nature and not restrictive.

Claims

We claim:

1. A method of using a blockchain to provide identity verification of a user, comprising:
 - (a) presenting identification documentation related to the user to a verifier party;
 - (b) recording information from the identification documentation on the blockchain in an identity token authenticated by the verifier party;
 - (c) accessing the identity token to provide identity verification of the user.
2. The method of claim 1, wherein the identity information is controlled by a public/private key pair controlled by the user.
3. The method of claim 1, further comprising:
 - (d) presenting identification documentation related to the user to a verifier party;
 - (e) if the verifier party verifies the identification documentation and its relationship to the user, then recording on the blockchain a token that invalidates one or more previously recorded identity tokens pertaining to that user, and recording information from the identification documentation on the blockchain in a new identity token authenticated by the verifier.
4. The method of claim 1, wherein the verifier party does not record the identity token unless the verifier party authenticates the user by comparing one or more biometric characteristics of the user with information in the identification documents.
5. The method of claim 1, wherein the identification documentation comprises documentation of name, birth date, residence address, professional license, academic certification, social security or other government identification, passport, photograph, manual signature, group membership, or a combination including one or more of those.
5. A method of verifying the identity of a user, comprising:
 - (a) presenting documentation of identity to a verifier party, and recording on the blockchain an identity token authenticated by the verifier party, where the identity token contains information from or related to the documentation;
 - (b) repeating step (a) one or more times, each time with different documentation, a different verifier party, or both, resulting in a plurality of identity tokens recorded on the blockchain;
 - (c) accessing one or more of the plurality of identity tokens to verify one or more characteristics of the identity of the user for a subsequent operation.
6. The method of claim 5, wherein step (c) comprises verifying from the identity tokens one or more of the name, birth date, age, residence address, professional license, academic certification, social security or other government identification, passport, photograph, manual signature, or group membership of the user, or the identity or verification of the verifier party that recorded the identity token.
7. The method of claim 6, wherein step (c) comprises verifying two or more of the characteristics listed in claim 6.

8. The method of claim 5, wherein the plurality of identity tokens are associated with a single wallet on the blockchain.
 9. The method of claim 5, wherein one of the identity tokens contains information that is correlated with information in another of the tokens.
 10. The method of claim 9, wherein verifying one or more characteristics of the identity of the user comprises verifying correlated information in a plurality of the identity tokens.
 11. The method of claim 10, wherein the subsequent operation comprises one or more of presenting information only if the verified characteristic satisfies a predetermined criteria, allowing a purchase only if the verified characteristic satisfies a predetermined criteria, allowing an entry to be recorded on the blockchain only if the verified characteristic satisfies a predetermined criteria, allowing the user to enter a facility only if the verified characteristic satisfies a predetermined criteria, or allowing the user to access an item only if the verified characteristic satisfies a predetermined criteria.
 12. A method of implementing a smart contract on a blockchain, processed by a plurality of validators, comprising checking as part of the validation process that one or more identity tokens, recorded on the blockchain using the method in any of claims 1-11 and corresponding to one or more of the parties to the smart contract, satisfy a predetermined criteria.
- Identity management in the present invention can include several operational steps such as identity verification by a third party, identity inquiries, and inquiry approval by the identity holder.