

METHOD OF MANAGING ROLE-BASED DIGITAL RIGHTS IN A

COMPUTER SYSTEM

TECHNICAL FIELD

[0001] The present technology relates generally to computer
5 systems and, in particular, to computer-implemented techniques
for role-based management of digital rights.

BACKGROUND

[0002] Role-based access control (RBAC) is a technique for
controlling access to a computer system or network. In an
10 organization's computer system, each user is assigned a role
or function (hereinafter "role"). User access rights or
permissions to perform tasks within the computer system are
assigned to the roles. RBAC thus provides a framework for
assigning user access rights and permissions based on the
15 roles, and not directly based on the identity of the users per
se.

[0003] In a conventional RBAC implementation, however, there
is no correlation between an assigned role in the computer
system and a real-world legal authority to perform an action
20 on behalf of the organization. A user may occupy a role X
that electronically permits him to perform a task Y in the
computer system but there is nothing in a conventional RBAC
implementation to guarantee that the performance of task Y by
the user in role X actually is authorized and/or that it has
25 any legal effect.

[0004] While electronic signatures may cryptographically
provide identification and non-repudiation mechanisms, there
is no way to ascertain that an electronic signature, or other
electronic transaction or digital act performed by a user
30 occupying a given role is actually legally authorized. The

legal authority of the user occupying a given role has to date been overlooked by RBAC systems.

[0005] This issue has implications not only in terms of internal corporate governance but also in the realm of e-commerce, especially in an international e-commerce transaction between distant organizations in which one user of a first organization may not be able to readily ascertain that another user of a second organization actually has authority to bind the second organization.

[0006] One e-commerce solution for role-based authorization is disclosed in U.S. Patent Application Publication 2001/0021928 (Ludwig et al.) entitled "Method for Inter-Enterprise Role-Based Authorization" that uses role certificates to enable one user from a first organization to authenticate another user from a second organization. However, this technology does not purport to link a role to a real-world legal authority to act on behalf of an organization.

[0007] Such a solution is disclosed in the present specification and the appended drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] Further features and advantages of the present technology will become apparent from the following detailed description, taken in combination with the appended drawings, in which:

[0009] FIG. 1 is a schematic depiction of a computer system for managing role-based digital rights in accordance with embodiments of the present invention;

[0010] FIG. 2 is a flowchart outlining main steps of a method of managing role-based digital rights;

[0011] FIG. 3 is a flowchart outlining main steps of a method of e-commerce;

[0012] FIG. 4 is an example of a registration authority (RA) verification page;

5 [0013] FIG. 5 is an example of a subsequent RA verification page;

[0014] FIG. 6 is an example of an RA checklist;

[0015] FIG. 7 is an example of a role manager screen that the RA uses to assign a role to a user;

10 [0016] FIG. 8 is an example of an e-commerce transaction dashboard;

[0017] FIG. 9 is a schematic depiction of a computer system for conferring legal authority to avatars that represent users within a computer-generated virtual world; and

15 [0018] FIG. 10 is a flowchart depicting steps of a method of conferring legal authority to avatars that represent users within a computer-generated virtual world.

[0019] It will be noted that throughout the appended drawings, like features are identified by like reference
20 numerals.

SUMMARY

[0020] In general terms, the present invention provides a novel computer system, computer-implemented method, and computer-readable medium for managing role-based digital
25 rights. The embodiments of the present invention implement an innovative paradigm for defining roles in the computer system that rely directly or indirectly on a registration authority who is licensed by a licensing body to ascertain the identity

of any legal entity such as an organization or person. For the purposes of this specification, the term "ascertain" shall be understood to describe the process of verifying the information that enables the registration authority to
5 ascertain the legal status of an entity or the identity of an individual. Furthermore, the present specification shall use the term "verify" in a broad sense to encompass the concept of ascertaining. The paradigm ensures that every registered user of the system has been duly ascertained by a registration
10 authority. The users may then be assigned roles by the registration authority which confer rights or permissions to undertake certain acts in the system. Any action by the user within the system is presumed to be legally valid as the authority of the user derives ultimately from the registration
15 authority. This creates a chain of trust originating from a registration authority to a verified user of the system. Because of the chain of trust, other users of the system may presume that the acts of a given user is valid and enforceable. This chain-of-trust paradigm transposes onto a
20 digital platform the real-world process of verifying each user's identity and ascertaining that the user's role confers proper authority to take certain acts. This technology greatly facilitates acts that are internal to the organization (e.g. resolutions, shareholder votes, or other internal
25 governance processes) and also acts that are external to the organization (e.g. tendering, procurement, contracting). This technology also greatly facilitates transactions in a virtual world.

[0021] With this in mind, there are a number of aspects of
30 the present invention that will be described.

[0022] One aspect of the present invention is a computer-implemented method of managing role-based digital rights in a computer system. The method entails (i) verifying a legal

status of a first user seeking to act as a registration authority by sending a status verification request to a licensing body server that stores status information regarding the legal status of the first user to ascertain that the first user is licensed to act as the registration authority; (ii) verifying a legal status of an organization having a hierarchical structure of roles by sending a status verification request to a status verification server that stores status information regarding the legal status of the organization verified by the registration authority or by any other registration authority deriving authority from an original registration authority; (iii) receiving user input from the registration authority to create an account for the organization within a document-interaction and transaction management application that enables interaction with electronic documents securely stored in a virtual vault and electronic transactions to be performed for the organization; (iv) verifying a legal status of a first member of the organization by sending a status verification request to the status verification server, the first member having been verified by the registration authority or by any other registration authority deriving authority from the original registration authority, wherein the registration authority also verifies that the first member has a legal capacity to act in the first role; and (v) receiving user input from the registration authority to define a first role within the organization for the first member, the first role conferring a first authority to act on behalf of the organization, wherein the first authority of the first member is predicated on the registration authority.

[0023] Another aspect of the present invention is a computer readable medium upon which are stored instructions in code that are configured to perform the steps, acts or operations

of the foregoing method when the computer readable medium is loaded into memory and executed on a processor of a computing device.

[0024] Yet another aspect of the present invention is a
5 computer system for managing role-based digital rights, the system comprising (i) an application server having a processor operatively coupled to a memory to execute a document-interaction and transaction management application that enables interaction with electronic documents securely stored
10 in a virtual vault and electronic transactions to be performed for the organization; (ii) a licensing body server for verifying a legal status of a first user seeking to act as a registration authority by receiving a status verification request and for that stores status information regarding the
15 legal status of the first user to ascertain that the first user is licensed to act as the registration authority; and (iii) a status verification server for storing status information about organizations and members whose legal status has been verified by the registration authority or any other
20 registration authority deriving authority from an original registration authority, wherein the registration authority also verifies that the first member has a legal capacity to act in the first role. The application executing on the application server is programmed to send a status verification
25 request to the licensing body server to verify the status of the registration authority, send a status verification request to the status verification server to verify a status of an organization, receive user input from the registration authority to create an account for the organization within the
30 application, send a status verification request to the status verification server to verify a status of a first member of the organization, and receive user input to define a first role within the organization for the first member, the first

role conferring a first authority to act on behalf of the organization, wherein the first authority of the first member is predicated on the registration authority.

[0025] The invention may also be used to facilitate e-commerce between two organization that are using the document-interaction and transaction management application as a common platform. The application mediates the transaction to ensure that members of each organization have authority to bind their respective organizations.

[0026] Accordingly, one aspect of the present invention is a computerized method of e-commerce between a first organization and a second organization each having a hierarchical structure of roles defined within a common document-interaction and e-commerce transaction application hosted in a distributed computing environment, wherein the roles confer different authorities to transact on behalf of the respective organizations. The method comprises receiving user input from an offering member of the first organization requesting that the document-interaction and transaction management application generate an electronic contract document representing an offer to enter into a contract, verifying by the application that the offering member of the first organization occupies a role having authority to contractually bind the first organization with respect to the contract, the role having being defined by a first member whose status has been verified by a registration authority, wherein the registration authority also verifies that the first member has a legal capacity to act in the first role. The method then involves generating the electronic contract document and permitting the first member to electronically sign the document only if the offering member has the authority to contractually bind the first organization with respect to the contract. The method then entails receiving user input

identifying an accepting member who is to receive the electronic document at the second organization. The method includes verifying by the application that the accepting member occupies a role conferring authority to accept the offer on behalf of the second organization, the role being defined by a second member whose status has been verified by a registration authority. Finally, the method includes transmitting the electronic contract document from the offering member of the first organization to the accepting member of the second organization if the accepting member has the authority to accept the offer, receiving user input from the accepting member of the second organization to electronically sign the document to accept the offer, and transmitting an electronic acceptance of the contract to the offering member of the first organization.

[0027] Another aspect of the present invention is a computer readable medium upon which are stored instructions in code that are configured to perform the steps, acts or operations of the foregoing method when the computer readable medium is loaded into memory and executed on a processor of a computing device.

[0028] Another aspect is a computer system for e-commerce, the system that includes an application server having a processor coupled to a memory for executing instructions in code of a document-interaction and transaction management application to facilitate e-commerce between a first organization and a second organization each having a hierarchical structure of roles conferring different authorities to transact on behalf of the respective organizations. The system includes a first computing device for receiving user input from an offering member of the first organization requesting that the application generate an electronic contract document representing an offer to enter

into a contract. The application is programmed to verify that the offering member of the first organization occupies a role having authority to contractually bind the first organization with respect to the contract, the role having been defined by
5 a first member whose status has been verified by a registration authority, wherein the registration authority also verifies that the first member has a legal capacity to act in the first role. The application is further programmed to generate the electronic contract document and permit the
10 offering member to electronically sign the document only if the offering member has the authority to contractually bind the first organization with respect to the contract. The first computing device further receives user input identifying an accepting member who is to receive the electronic document
15 at the second organization. The application is programmed to verify that the accepting member occupies a role conferring authority to accept the offer on behalf of the second organization, the role having been defined by a second member whose status has been verified by a registration authority.
20 The application is then programmed to transmit the electronic contract document from the offering member of the first organization to the accepting member of the second organization if the accepting member has the authority to accept the offer. The system includes a second computing
25 device for receiving user input from the accepting member of the second organization by electronically signing the document to accept the offer. The application is then programmed to transmit an electronic acceptance of the contract to the offering member of the first organization.

30 **[0029]** The present invention also has applicability to virtual worlds. The present invention may be used to confer legal authority on avatars interacting in a virtual world. Yet another aspect of the present invention is a computer-

implemented method of conferring legal authority to avatars that represent users within a computer-generated virtual world in which the users interact with each other via their respective avatars. The method comprises verifying a legal
5 status of a registration authority by sending a status verification request to a licensing body server to ascertain that the registration authority is licensed to act as the registration authority; verifying a status and capacity of a user seeking to become a member of the virtual world by
10 sending a status verification request to a status verification server that stores status information regarding the legal status of the user and the legal capacity to become a member of the virtual world, wherein the legal status and legal capacity have been verified by the registration authority or
15 by any other registration authority deriving authority from an original registration authority; and receiving user input from the registration authority to create an account for the member within the virtual world, the account linking the member to a unique avatar, wherein the authority of the avatar in the
20 virtual world is predicated on the registration authority.

[0030] The details and particulars of these aspects of the invention will now be described below, by way of example, with reference to the attached drawings.

DETAILED DESCRIPTION

25 **[0031]** In general, the embodiments of the present invention relate to a novel computer system, computer-implemented method, and computer-readable medium for managing role-based digital rights. The embodiments of the present invention implement an innovative chain-of-trust paradigm that employs
30 registration authorities (e.g. lawyers) who are licensed by a licensing body (e.g. a state or provincial bar) to verify the identities of persons wishing to become system users.

[0032] One or more original (seminal) registration authorities may create additional registration authorities by verifying the identity of each of those additional registration authorities who may, in turn, create further
5 registration authorities. As a result, a group of registration authorities will be required for any given jurisdiction in which the system is to be deployed.

[0033] A person wishing to register as a user of the system must have his or her identity verified by one of these
10 registration authorities. Only if the person's identity has been duly verified by the registration authority may a user account be created and/or the user added to a user database as a known entity. Similarly, an entity or organization (e.g. a corporation) must be verified (in terms of its legal status)
15 by a registration authority before an account for the organization is created in the system. Accordingly, only entities that have been verified by a registration authority may access and utilize the system. The platform is thus restricted to entities whose identities have been formally
20 verified by registration authorities having a statutory power of certification. The user may then be assigned a role in an entity or organization. The role determines a set of rights, permissions, privileges, etc. within the document-interaction and transaction management application, as will be explained
25 in greater detail below. As a precondition for assigning a role to a registered user, the system verifies that the user is entitled (has legal capacity) to occupy that role. This decision may be made by the RA or by the system by comparing attributes of the user with legal requirements for the role.

30 [0034] Although the primary application of this technology is to an organization such as a corporation having a hierarchical set of roles within a pre-existing legal framework, the technology may also be used or adapted to manage digital

rights with respect to any entity, where an entity is understood broadly to encompass a body corporate, trust, partnership, foundation, unincorporated association, group or any such organization, as well as a government, agency, bureau, office, department or ministry of the government. In one embodiment, the entity may also include a natural person (i.e. an individual) who has the legal capacity to delegate authority to another person within a certain legal framework, e.g. granting a power of attorney. For example, a natural person User A (who is a verified registered user) may grant a power of attorney to another person User B (who is also a verified registered user). The identities of User A and User B are verified by one or more registration authorities. The system may also, in some limited cases, verify some invariant elements of User A's legal capacity to grant the power of attorney and of User B's legal capacity to accept the power of attorney. The system thus can provide some basic information regarding legal capacity such as age that help ensure that actions taken by User B when exercising the power of attorney are legally valid and binding on User A. The system also ensures that a third party (User C) interacting with User A may rely on the authority granted to User B. This example demonstrates how an entity may be a natural person.

[0035] SYSTEM

[0036] FIG. 1 schematically depicts a computer system in accordance with an embodiment of the present invention. This computer system has two main components: (i) an authentication and status verification server (SVS) and its associated user database whose general function is to authenticate users and (ii) a document-interaction and transaction management application whose general function is to provide authenticated users with a software interface for interacting with documents and performing electronic actions and tasks with respect to an

organization of which the user is a member having an assigned role.

[0037] As depicted by way of example in FIG. 1, a plurality of users who are designated by reference numerals 10, 20, 30
5 communicate with the computer system over a data network, e.g. Internet 50, using wired or wireless digital data communication technology. For the sake of illustration, three such users (User1, User2, and User3) are depicted by way of example in FIG. 1 although the number of users may vary.
10 Again for the sake of illustration, User1 connects to the system via the Internet 50 using a desktop computer 12, User2 connects to the system via the Internet 50 using a laptop 22 and User3 connects to the system via mobile device 32 communicatively connected to the Internet via a wireless
15 network and gateway. Standard communication protocols, such as TCP/IP, HTTP, etc may be used to connect to the system through the Internet.

[0038] The mobile device 32 may be any wireless communication device, smart phone, cell phone, wireless-enabled PDA,
20 wireless-enabled tablet, or other portable or handheld electronic device that has wireless communication capabilities. The mobile device 32 may connect wirelessly to the system via wireless network (represented schematically by base station tower 40) using any known cellular technologies
25 or communication protocols such as, for example, GSM, EDGE, LTE, CDMA, etc. Other wireless technologies may of course be employed such as, for example, Wi-Fi™, Bluetooth®, satellite link, etc.

[0039] As depicted in FIG. 1, the users connect to Web
30 interface servers 60, 70 which are respectively connected via firewalls 62, 72 to an authentication and status verification

server (SVS) 80 and to a document-interaction and transaction management server (DITMS) 90.

[0040] As depicted in the exemplary architecture shown in FIG. 1, the SVS 80 and the DITMS 90 are both connected to a common ID and security server 100 (hereafter referred to simply as an "identification server").

[0041] SVS

[0042] The SVS 80 receives and processes authentication requests from registered users. If the user is registered and authenticated, e.g. by multi-factor authentication sufficient to establish that the user is who he purports to be, access to the system is granted. The SVS 80 also stores user profile information for each registered user. In another embodiment, the authentication and verification functions may be decoupled and performed by physically distinct servers.

[0043] The SVS 80 is consulted or queried by the DITMS when it is necessary to ascertain that the user is registered with the system and has a proper status. In other words, the DITM application relies on the SVS to ensure that users of the application are registered users that have been duly verified by a registration authority. The SVS guarantees that the users of the DITM application are registered users whose electronic identities can be trusted. In one implementation, the SVS may be replaced by an entity status verification system that stores entity status information once entities have been duly verified by an RA.

[0044] LB-SVS

[0045] In the implementation illustrated in FIG. 1, the SVS 80 is further configured to communicate with a licensing body status verification server 84. The licensing body status

verification server (LB-SVS) may be a professional organization web services or other system that stores status information of registration authorities. The LB-SVS is thus consulted when it is necessary to ascertain that a user who is acting as a registration authority is a member in good standing of the licensing body and thus legally entitled to act at that moment in time as a registration authority. For example, the professional licensing body may be a state or provincial bar that regulates and licenses lawyers. The roster of lawyers who are members of a state or provincial bar is supplemented with continually updated status information so that the system can ascertain that a lawyer seeking to act as a registration authority is still, at that moment in time, in good standing.

15 **[0046]** DITMS

[0047] The document-interaction and transaction management server (DITMS) 90 may execute a document-interaction and transaction management (DITM) application hosted by the DITMS 90. The DITM application provides a panoply of functionalities permitting system users to access and interact with documents in the document vault (secure virtual vault 92). For the purposes of this specification, interacting with documents shall be understood in a broad sense to mean acts, actions, activities, transactions, or tasks performed in relation to a document such as, but not limited to, opening, accessing, viewing, creating, editing, annotating, commenting, highlighting, deleting, cutting, copying, pasting, importing, exporting, e-mailing, archiving, voting, approving, etc. Thus, the DITM application enables a user to perform a plurality of functions on the documents and data in the secure vault.

[0048] In one example, the organization may be a corporation. Its important corporate documents such as its minute book, articles of incorporation, corporate bylaws, resolutions, shareholder agreements, security offerings, etc. are stored in electronic form in the vault. Access to these documents by the corporation's directors, officers, employees, external lawyers, accountants, etc. is controlled by assigning to each user a role within the corporation account in the application. Thus, the role of director may confer much greater access rights than the role of mere employee.

[0049] In addition to document-related interactions, the DITM application enables the user to perform and manage transactions. Transactions are meant to broadly encompass any external business activities (e.g. contracting with other organizations using the same DITM software platform, filing tax returns, filing documents for securities compliance or with any other government or regulatory agency, etc.) or any internal activities of the organization (e.g. governance-related activities, such as resolutions, votes, approvals, appointments, shareholder agreements, additions to the minute book, etc.) such as, either internally within the organization or externally with another organization, or even within a virtual world.

[0050] The DITM application enables these various actions to be performed by a user occupying a role that confers the authority to perform the action. In other words, the access rights, usage rights, permissions, and privileges accorded to a given user are determined by the role assigned to the user within the organization. The role for the first member or plurality of first members is defined by the registration authority. Subsequently, the first member may create a subsidiary (second) role for a second member by exercising a derivative role-creation right provided such a right was

conferred on the first member by the RA. The second member may create a third role for a third member if the second role has its own derivative role-creation right. As will be appreciated, any number of subsidiary roles may be created in a hierarchical chain that originates with the registration authority. Each member in the chain must be a system user who has been verified by an RA. The authority of a member is thus linked to (or predicated on) the registration authority.

[0051] The DITM application may be stored on and executed by a single server machine (computing device) as shown by way of example in FIG. 1 or, alternatively, it may be stored on and executed separately by a server cluster or in a cloud-computing environment. The DITMS 90 that runs the DITM application may be physically distinct from the secure document vault 92 or these may be consolidated as a single machine. In other embodiments, there may be multiple servers 90 and/or multiple vaults 92, e.g. to segregate data by jurisdiction.

[0052] Each server (computing device) may include one or more processors (or microprocessors), memory (hard disk drive, solid state drive, etc.), one or more data buses, communications ports and input/output devices.

[0053] The SVS 90 and the DITMS 90 together provide a virtual platform for authenticating users and for permitting the users to interact with digital documents stored in a virtual vault or to perform digital transactions with respect to the organization of which the users are members. The DITMS 90 queries the SVS to verify the status of a user of the DITM application when that user is to be assigned a role. Only if the status verification is OK does the DITMS assign a role to the user. In most embodiments, the DITMS and/or the SVS communicates directly or indirectly with the LB-SVS to verify

a status of an RA when the RA performs an operation in the DITM application.

[0054] System Operation and Interaction

[0055] Prior to accessing the system, each user must become a
5 registered user of the system. As noted above, a person
seeking to become a registered user of the system must be
verified by a registration authority, e.g. a lawyer in good
standing with his state or provincial bar. After the person
has been duly verified by a registration authority in the
10 manner prescribed by law, the registration authority may then
create a user account for the user to access the system. The
user account, which may contain user profile information and
optionally any cryptographic material assigned to the user,
may be stored at the status verification server (SVS) 80 or
15 its associated user database 82. In one embodiment, the
cryptographic material may include user-specified credentials
known only to the user.

[0056] As part of the user account creation process for the
newly verified user, a status verification request is sent to
20 the LB-SVS 84 to ascertain that the registration authority is
himself a member in good standing with the licensing body and
that he has full and complete capacity to verify and vouch for
the identity of the new user. The continually updated status
of each registration authority is thus stored in one of a
25 plurality of licensing body status verification servers
(generally one per jurisdiction) which may be queried in real-
time by a web interface to ascertain that the registration
authority still has legal capacity to act as a registration
authority, e.g. that the lawyer has not been disbarred,
30 suspended or has otherwise lost his license to practice.

[0057] The registration authority thus adds the user to the user database 82 of users who have been duly verified by a registration authority. In like manner, an organization such as a corporation, limited partnership, trust, etc. may be verified by a registration authority and added to the database 82. The database 82 may thus store any entity, be it a corporation, natural person, etc. Each registration authority (RA) must have within its jurisdiction the legal capacity to verify the identity of an entity such as an organization (e.g. a corporation, limited partnership, trust, etc) or a natural person. Once verified by an RA, an account or profile for the organization or person may be created in a database 82 associated with the SVS 80. A cryptographic key, certificate or token may be associated with the user account or organization account. In this manner, the SVS maintains a database of verified entities (organizations and users) who have been duly verified by a registration authority and are thus unique in the system. The user account or profile may contain information, data or parameters indicating the legal capacity of the user to take on various roles. The RA can then assign a role to the registered user after ensuring that the user has the full legal capacity to act. The RA then grants authority to the user by assigning the role to the user. This grant of authority from the RA to the first member can only be done if the first member is verified and has legal capacity to act in the role. This is the first link in the chain of trust.

[0058] To summarize, the computer system includes an application server (DITMS 90) having a processor operatively coupled to a memory to execute a document-interaction and transaction management (DITM) application. This application enables interaction with electronic documents securely stored

in a virtual vault 92 and electronic transactions to be performed for the organization.

[0059] The system includes a licensing body server (LB-SVS 84) for verifying a legal status of a first user seeking to act as a registration authority. The LB-SVS receives a status verification request from the SVS or DITMS. The LB-SVS stores status information regarding the legal status of registration authorities. The LB-SVS thus acts to ascertain that the first user who purports to be a registration authority is currently licensed in that jurisdiction to act as the registration authority.

[0060] The status verification server (SVS 80) stores status information about organizations and members whose legal status has been verified by the registration authority or any other registration authority deriving authority from an original registration authority.

[0061] The DITM application executing on the DITMS 90 is programmed to (1) send a status verification request to the LB-SVS 84 to verify the status of the registration authority; (2) send a status verification request to the SVS 80 to verify a status of an organization; (3) receive user input from the registration authority to create an account for the organization within the application hosted by DITMS 90; (4) send a status verification request to the SVS 80 to verify a status of a first member of the organization and (5) receive user input at DITMS 90 to define a first role within the organization for the first member. The first role confers a first authority to act on behalf of the organization. The first authority is thus predicated on the registration authority. In embodiments of the invention, the registration authority also verifies that the first member has a legal capacity to act in the first role. This ensures that the

first member is legally entitled to occupy the first role, unlike conventional RBAC systems which do not take into consideration the legal capacity of a user to occupy a given role. By verifying the legal capacity of a user to act in a given role, the system imposes an actual legal framework on the users of the system. The system can thus act as an auditing mechanism which can be employed to prove *ex post facto* that users acted in accordance with the legal requirements at the time a given act was undertaken in the system.

[0062] The document-interaction and transaction management (DITM) application thus provides a virtual platform for interacting with digital documents of an organization that are securely stored in a virtual vault and for performing electronic acts or transactions for, or on behalf of, the organization. The acts may be internal acts relating, for example, to the internal governance of the organization or external acts relating, for example, to contracts entered into with other organizations. Permissions for these acts are based on the roles assigned within the organization. Each role is defined to have a legal authority (i.e. power or capacity) to perform one or more tasks, acts, actions or transactions. Each role derives its legal authority ultimately from a registration authority.

[0063] In other words, the status of a registration authority (RA) is verified by sending a status verification request to a licensing body server, e.g. LB-SVS 84. The RA then verifies the legal status of an organization and of a first member (or of a plurality of first members) of the organization. Authorities conferred on a member are thus predicated on the registration authority. This creates a chain of trust linking the authority of a member of the organization to the registration authority. This paradigm imposes the real-world

legal requirements for verifying identities on the system. As a consequence, the system guarantees that there is legal authority for an electronic action performed within the system by a user occupying a role that was granted through a chain of trust by a registration authority.

[0064] Roles in the computer system are defined such that they rely directly or indirectly on a registration authority who is licensed by a licensing body to verify the identity of any legal entity such as an organization or person. This paradigm ensures that every registered user of the system has been duly verified by a registration authority. The users may then be assigned roles by the registration authority which confer rights or permissions to undertake certain acts in the system. Any action by the user within the system is presumed to be legally valid as the authority of the user derives ultimately from the registration authority. This creates a chain of trust originating from a registration authority to a verified user of the system. Because of the chain of trust, other users of the system may presume that the acts of a given user is valid and enforceable. This chain-of-trust paradigm transposes onto a digital platform the real-world process of verifying each user's identity and ascertaining that the user's role confers proper authority to take certain acts. This technology greatly facilitates acts that are internal to the organization (e.g. resolutions, shareholder votes, or other internal governance processes) and also acts that are external to the organization (e.g. tendering, procurement, contracting).

[0065] The system architecture depicted in FIG. 1 is presented as one example implementation. It will be appreciated that the system may be implemented with other architectures by consolidating or distributing the various

server functions. It will also be appreciated that the system may be implemented in a cloud-computing environment.

[0066] METHOD OF MANAGING ROLE-BASED RIGHTS

[0067] This technology enables a computerized method of
5 managing role-based rights within an organization that has a
hierarchical structure of roles such as a corporation. The
method involves verifying the registration authority, and then
verifying the identity of the user who is to be assigned a
role within an organization (by checking that the user is
10 registered in the SVS as a person whose identity has been
verified by an RA) and also verifying the legal capacity of
that user to act in the role to be assigned. Such a method
creates a chain of trust that ensures that the member
appointed to the role within the organization has been
15 appointed in accordance with legal requirements imposed in
that jurisdiction.

[0068] For clarity, it is to be understood that this method
is presented from the perspective of the DITM application as a
user creates an organization, selects users to become the
20 members of that organization, and then assigns roles to these
members. This would be the case when a corporation account is
created in the application by a registration authority. As a
prerequisite, the legal status of the corporation must be
verified. The users who are to be selected as the members of
25 the organization must also be verified. The members must then
be assigned roles, e.g. as directors, officers, shareholders,
employees, etc. within the corporation. The method begins
when a first user (e.g. a lawyer) who purports to be a
registration authority (RA) wishes to create the organization
30 account within the DITM application. The first user as an
ostensible RA logs into the system and requests creation of an
organization account, e.g. an account for a client

corporation. The system will verify initially that the first user (the lawyer) is currently still a valid RA. To do so, his status is checked with the LB-SVS 84 (e.g. the professional status database maintained by his state or provincial bar).

[0069] The method thus depicts in FIG. 2 an initial step 200 of verifying a legal status of a first user seeking to act as a registration authority. This is done by sending a status verification request through the network to a licensing body server (LB-SVS) that stores status information regarding the legal status of the first user. The status verification request may be a message or datagram in a predefined format that specifies the name and/or professional license registration number of the user. The LB-SVS executes software that is programmed to recognize the predefined format and automatically search and obtain the status information. This status verification request ascertains whether the first user is licensed to act as the registration authority (RA). Assuming the first user is a valid RA, the application then allows the RA to act. The RA may thus request that the SVS be queried as to whether the corporation in question is a known entity (i.e. whether the corporation has already been verified by an RA). This verification may have been performed by the RA himself or previously by another RA, i.e. any other RA deriving authority from an original RA. In any event, the corporation's identity (legal status), if it's been verified by an RA, has been entered into the SVS database. The DITM server queries the SVS to verify that the corporation is a known entity. Thus, at step 210, a legal status of an organization is verified by sending a status verification request to the SVS. Assuming that the corporation is known to the SVS because it has been previously verified, an affirmative status reply is communicated back to the DITMS

from the SVS. The RA is then able to create an account for the organization within the DITM application.

[0070] Accordingly, at step 220, the method involves receiving user input from the RA to create an account for the organization within the DITM application.

[0071] The RA will then assign a role to a selected user who is a first member of the organization. To do so, the DITM queries the SVS to ascertain that the selected user is a known entity, i.e. that the selected user has been verified by an RA and that the user has the capacity to take on the role to be assigned.

[0072] Accordingly, at step 230, the system verifies a legal status of the first member of the organization by sending a status verification request to the SVS. Assuming the first member has been verified by an RA, the SVS will reply with an acknowledgement that the first member is known. The RA can then assign a role within the organization to the first member because the first member has been verified. The registration authority also verifies that the first member has a legal capacity to act in the first role. For example, the first role may be a director of a corporation. In a given jurisdiction, there may be requirements that the director be a resident, be of the certain minimum age, etc. These requirements are verified by the RA prior to assigning this role to the member. The verification of the legal capacity to assume a role may also be automated by the system. In one embodiment, the system compares attributes of the user from the user account or user profile with a set of rules, parameters or requirements that reflect the legal requirements of the role. For example, the role may require that the user be a citizen or resident of the jurisdiction, that the user have no criminal record, that the user be of a minimum age,

that the user have a professional status, degree, certification, elected status, appointed status, delegated status, etc. These attributes can be entered into the user account within the user database 82. These personal
5 attributes form part of the user's profile. These attributes may be input and verified when the RA verifies the user's identity. The system can then automatically query the user database to compare the attributes with the requirements.

[0073] Therefore, at step 240, the application receives user
10 input from the RA to define a first role within the organization for the first member. The first role confers a first authority to act on behalf of the organization. The first authority is thus predicated on the registration authority.

[0074] A further optional step 250 comprises receiving user
15 input from the first member to create a second role for a second member in compliance with internal governance rules that are determined by legal requirements imposed on the organization, the second role conferring a second authority to
20 act on behalf of the organization, thereby creating a chain of trust that predicates the second authority of the second role on the first authority of the first role which, in turn, is predicated on the status verification of the registration authority. The internal governance rules, e.g. a majority-
25 rule system for a board of directors, is imposed on the first members by the RA, requiring that any action the first member take comply with the legal framework imposed on the first members. The first members may agree (by majority vote) to change the internal governance rules but this vote is
30 constrained by the original legal framework imposed by the RA in accordance with the law of the jurisdiction governing the organization. Any statutory, regulatory, or other legal requirements for an organization within a given jurisdiction

may be programmed into the system as rules or parameters governing how the members may act. In other words, a hierarchy of roles may be created within the organization, each obtaining its authority from the previous role. In that
5 sense, a role may be understood as conveying a set of rights, one right being the right to create a role. Each role (and its authority) can thus be traced back through the hierarchy to the first member(s) of the organization who received his authority from the registration authority. This is termed the
10 chain of trust.

[0075] In one implementation, the SVS (or one or more applications, modules or the like executing on the SVS) guides the RA through the verification process by displaying (e.g. via a Web interface of the SVS) the legal requirements to
15 perform a verification as mandated by law in a given jurisdiction. In most embodiments, the SVS stores the legal verification requirements for each of a plurality of different jurisdictions for each of a plurality of different types of entities that may be created in the system. In other words,
20 the SVS stores in memory the verification requirements that are displayed to the RA when the RA specifies the type of entity and the jurisdiction. The verification requirements thus serve as a guide or tool in performing the requisite steps for verifying an entity. The requirements are drawn
25 from the legal framework (e.g. the laws, statutes, regulations, codes, bylaws, etc., governing the constitution of an entity in a given jurisdiction.

[0076] An example of the legal framework is, for example, Article 335 of the Civil Code of Quebec which reads: The board
30 of directors manages the affairs of the legal person and exercises all the powers necessary for that purpose; it may create management positions and other organs, and delegate the exercise of certain powers to the holders of those positions

and to those organs. The board of directors adopts and implements management by-laws, subject to approval by the members at the next general meeting. The legal person may be, for example, a corporation, trust, etc. From this framework follows the authority of the board and the capacity to create management positions and to delegate the exercise of certain powers. The present system provides a digital platform that replicates the general legal framework for each type of entity for each jurisdiction.

10 [0077] In one implementation, the SVS determines the jurisdiction in response to user input from the RA, determines the type of entity also in response to user input from the RA and then presents to the RA a checklist of acts that the RA must perform in order to comply with the verification requirements, i.e. in order to properly verify that the organization or entity has been duly constituted or created. The RA then clicks on the various boxes of the checklist to indicate that he has performed each of the required verifications. The verification checklist is generated automatically by the SVS based on the type of entity and the jurisdiction governing the entity. In addition or in lieu of the checklist, the SVS may display fields for data entry, requiring that the RA enter data or information collected from the entity. For example, the SVS may require the RA to enter a corporation number and a passcode. The SVS will then query a corporate registry or other government database to determine if the corporation number and passcode are correct. Similarly, the SVS may require the RA to enter the names of all directors and their social security numbers (or social insurance numbers). The SVS can then verify this data by querying a government database. These are simple examples to illustrate how the SVS may challenge or test the RA to ensure that the RA is engaging in a full and complete verification.

[0078] Optionally, the SVS may store electronic copies of any supporting documents (e.g. scans of photo ID cards, passports, digital fingerprints, voice prints or other biometrics, digitally signed certificates from corporate registries, etc.)

5 that the RA has used in verifying the entity. This supporting data may be encrypted or non-encrypted in the SVS. Encryption may be used to control access to this data so that only one RA or a group of RA's has access to it.

[0079] Optionally, the SVS may perform conflict checks to ensure that the status of one organization does not conflict with another organization already registered in the system.

The SVS may display a warning if there is a conflict, in one embodiment, which the RA may manually override by providing suitable user input to the SVS. For example, the system may
15 flag a corporate name conflict between one entity in one jurisdiction and another entity in a different jurisdiction which would not have been identified by the corporation registries of each jurisdiction acting separately and alone.

[0080] In a similar vein, the SVS may optionally perform a conflict check to ensure that a user acting as a member of one
20 organization does not preclude the same user member from acting as a member of another organization. For example, a first organization may appoint a first member on condition that the first member devote all of his time and attention to
25 the affairs of the first organization. The SVS may warn the RA if he attempts to assign a role to that same first member in a second organization.

[0081] The method may further comprise a step of receiving user input from the second member to perform a restricted
30 action in the application, a step of verifying that the second member has requisite authority to perform the restricted action, and a step of performing the restricted action in the

application only if the second member has the requisite authority. The requisite authority depends on the role the user/member occupies.

[0082] The method may further comprise assigning a plurality
5 of first roles to a plurality of first members, the first
members being governed by a reconfigurable majority-rule
governance scheme. For example, in the case of a corporation,
the plurality of first members are the first directors.
Generally, the role of director is assigned a set of rights
10 and permissions. The directors are governed by a majority-
rule governance scheme. The directors can then vote to change
or reconfigure the governance scheme. All actions flow from
the initial framework that is instituted by the RA for the
corporation which replicates the real-world legal framework
15 for the corporation.

[0083] METHOD OF E-COMMERCE

[0084] This technology also enables a computerized method of
e-commerce between a first organization and a second
organization. Each organization has a hierarchical structure
20 of roles which confer different authorities to transact on
behalf of the respective organizations. The problem that
conventionally arises in e-commerce is that one party must
rely on ostensible authority of the other party. In other
words, there is no way to know with certainty and in a timely
25 manner whether the other party has the proper authority (i.e.
is legally entitled) to contractually bind his organization.
The capacity to act is typically a question of the user's role
within the organization. The present solution to this problem
is to have each organization share a common web-hosted
30 document-interaction and transaction management (DITM)
application that interfaces with the SVS. The DITM
application and the SVS cooperate to ensure that at a minimum

the organization and the members have been duly verified by a registration authority. Furthermore, the system ensures that roles have been assigned to the members by the registration authority in accordance with applicable statutory and regulatory requirements for the type of organization in question.

[0085] This computerized method thus enables a member of the first organization to know whether a member of the second organization actually has authority to act on behalf of the first organization.

[0086] With reference to FIG. 3, the method is initiated at step 300 when the DITM application receives user input from an offering member of the first organization. The offering member requests that the application generate an electronic contract document representing an offer to enter into a contract.

[0087] In response, at step 310, the application verifies that the offering member of the first organization occupies a role having authority to contractually bind the first organization with respect to the contract, the role having been defined by a first member whose status has been verified by a registration authority. The legal capacity of the member to occupy the role is also verified by the registration authority to ensure that the appointment of the member to that role is in conformity with any applicable legal requirements.

[0088] At step 320, the application generates the electronic contract document and permits the first member to electronically sign the document only if the offering member has the authority to contractually bind the first organization with respect to the contract.

[0089] At step 330, the offering member then provides user input identifying an accepting member who is to receive the electronic document at the second organization.

[0090] The application verifies that the accepting member occupies a role conferring authority to accept the offer on behalf of the second organization at step 340. The role has been defined by a second member whose status has been verified by a registration authority. In some embodiments, some elements of the legal capacity of the user to occupy that role has also been verified, either directly by the RA or by the system in response to input or a command from the RA.

[0091] At step 350, the application then transmits the electronic contract document from the offering member of the first organization to the accepting member of the second organization if the accepting member has the authority to accept the offer.

[0092] At step 360, the application then receives user input from the accepting member of the second organization who may electronically sign the document to accept the offer. Finally, an electronic acceptance is transmitted to the offering member of the first organization.

[0093] Because both organizations and their respective members have been verified by the SVS, there is presumed authority for the actions taken by each member on behalf of their respective organizations. This enables an e-commerce transaction to proceed without uncertainty as to whether the persons purporting to have authority to contract actually have the requisite authority to contractually bind their respective organizations. This computer system thus provides a web-based or cloud-based platform for e-commerce.

[0094] FIGS. 4 to 7 depict various examples of user interfaces ("screens" or "pages") that the system may present to enable the RA to perform the verification and role assignment tasks.

5 **[0095]** As shown by way of example in FIG. 4, a registration authority verification page 400 may include welcome information and an indication 410 that the RA's status is being automatically verified with the appropriate LB-SVS. Optionally, a location indication 420 of the detected current
10 location of the RA may be displayed along with a button 430 to correct this if the location information is incorrect. Optionally, an LB-SVS identifier 440 is displayed indicating which LB-SVS is being queried along with a correction button 450. This is useful for an RA who is a member in good
15 standing of two different licensing bodies for two different jurisdictions, e.g. the bar of New York and the bar of Quebec.

[0096] As shown by way of example in FIG. 5, a further registration authority verification page 500 may be displayed when the LB-SVS returns an affirmative status reply. The
20 welcome information 510 is updated. User interface elements 520, 530 are displayed to permit the RA to verify a user or organization.

[0097] As shown by way of example in FIG. 6, the system may present a registration authority checklist 600 for the RA to
25 guide the RA through the process of verifying an entity in a given jurisdiction. Jurisdiction information 610 and entity type information 620 may be presented. Optionally, checkboxes 630 may be provided for the RA to check when each condition has been verified. Optionally, a button 640 to view
30 applicable rules and requirements may be provided for each condition. Optionally, the screen 600 may include various task buttons 650, 660, 670, 680, 690 may be presented for

various tasks like finishing/signing, viewing supporting documents, importing supporting documents, requesting help, or cancelling the screen.

[0098] FIG. 7 is an example of a role manager screen 700 that permits the RA to assign a role to a registered user. Optionally, the screen 700 may depict RA information including the RA's name, status, LB-SVS, and last verification time and next verification time. The role manager screen 700 may optionally include a user interface element 720 to select a registered entity from the SVS database and a user interface element 730 to select a registered user from the SVS database who is to be assigned a role within the selected entity. Optionally, the screen 700 includes user interface elements 740, 750, 760 to verify the legal capacity of the user to occupy the role, to assign the role and to notify the user and/or entity of the role assignment.

[0099] In one implementation, the method entails displaying a transaction dashboard such as the one shown by example in FIG. 8. This e-commerce transaction dashboard 800 may in the illustrated embodiment display or otherwise present names and respective roles of all of the members that must electronically sign the document to be legally valid and further displaying a signature status indicating whether each member has signed the document. For example, as shown in FIG. 8, the dashboard 800 presents transaction description 810, a closing data, an internal reference number 820 to identity the transaction in question. Checkboxes 830 or other status indicators may display whether each required member has signed off on the transaction. A send reminder button (or other user interface element) 840 may be provided to send a reminder to a member who has not yet approved the transaction. The unchecked box 850 may be accompanied by a description that the system is awaiting signature from the member, as shown. An

automatic reminder system may also be provided to automatically communicate reminders to those members who have not yet signed off. Other buttons or user interface elements may be displayed such as a view documents button 860, a help
5 button 870 and a cancel 880. Additionally or alternatively, the dashboard may sequentially notify each of the members who must electronically sign the document in a predetermined order. This dashboard enables offering and accepting members to efficient manage the transaction by ensuring that all
10 members have signed off.

[00100] In one implementation, the method entails creating and sending a counteroffer to the first organization and determining if the offering member of the first organization still has authority to accept the counteroffer. The
15 counteroffer may, for example, be for a larger amount of money for which the offering member no longer has authority. This optional feature would check whether the terms of the counteroffer are still within the scope of the offering member's capacity to contract.

20 **[00101]** In one implementation, the method entails determining that the accepting member is non-responsive, determining whether the offer is time-limited, and automatically notifying another member whose role confers an equivalent authority to accept the offer. This feature enables the transaction to be
25 approved by another member if the original offering member or accepting member is unavailable for any reason, e.g. away on vacation, out of the office on business travel, on sick leave, etc.

[00102] APPLICABILITY TO LEGAL ACTS IN VIRTUAL WORLDS

30 **[00103]** In another implementation, the present technology may be adapted to a virtual world or virtual environment. A

virtual world is an online computer-generated game or simulation in which users interact with objects in their environment and with each other through their respective avatars. An example of a virtual world is Second Life™.

5 Commerce between avatars in the virtual world is conducted with a virtual currency which may have real-world value. For example, in Second Life™, virtual currency known as Linden dollars may be purchased with real-world US dollars. An avatar may earn or spend Linden dollars in the virtual world
10 and then redeem or exchange the Linden dollars for real-world US dollars. It is thus possible to make money in the virtual world. Commercial disputes that arise in the virtual world are difficult to resolve using traditional approaches (i.e. recourse to a court of law or alternative dispute resolution
15 mechanisms) because of a variety of legal issues such as questions of jurisdiction and the real-world identity of the avatar. Other legal issues (property ownership, torts, etc.) also cannot be easily resolved in a virtual world, primarily because of issues of identity. In other words, one of the
20 fundamental problems that arises in a virtual world is that the avatar cannot be easily legally linked to a real-world entity. The present technology addresses this basic problem by employing a registration authority to verify that a user is legally the virtual extension of the user. Once verified by
25 the RA, the user and his avatar are registered in the SVS or its associated user database.

[00104] An example of a generic web-based virtual world computer system is depicted in FIG. 9. The virtual world software engine (application) executes on a virtual world
30 server 900 (or server cluster or cloud). The virtual world server 900 may have an avatar database 930 (storing avatar information, attributes, properties, etc.) and a graphics database 940 (storing scene data for the virtual environments

that form the virtual world). The virtual world server 900 can require formal user registration with the SVS 80, which entails verification of the user by the RA and storage of the verified user information in the user database 82 in association with the user's unique avatar. User access to the virtual world can thus be controlled so that only known and registered users 10, 20, 30 whose identities have been duly verified by a registration authority can access the virtual world.

10 **[00105]** The computer system depicted in FIG. 9 therefore provides a virtual e-commerce platform or legal transaction management platform that is based on a modified version of the DITM application which is referred to herein in the context of a virtual world as a legal transaction management (LTM)
15 application. The LTM application executes on the legal transaction management server 910 and may include or be connected to a secure document vault 920 for securely storing contracts, digitally signed documents, or other such data. The LTM server 910 relies on a registration authority for
20 verifying the identity of the users 10, 20, 30 of the virtual world. Once verified, the user account at SVS database 82 legally links the users to their avatars. A certificate may be issued to enable users via their avatars to digitally sign contracts and to engage in formal legal acts in the virtual
25 world such as buying or selling property, entering into contracts of employment or service, entering into legal matrimony with another avatar, executing a last will and testament, etc. Any act taken by the user via his avatar in the virtual world will thus have a legal effect since the
30 avatar is legally connected to the registered user.

[00106] The SVS may be employed to store the registered users and the corresponding avatars. The DITM application may be adapted or transformed into a virtual-world legal transaction

management (LTM) application that interfaces with the virtual world game engine or game platform to provide an add-on platform or module for any legal transactions such as commercial contracts between avatars, virtual property-related transactions, formations of virtual corporations, etc. In other words, the legal transaction management application enables legally binding interactions and transactions between avatars within the virtual world. If a dispute arises between two avatars in the virtual world, the identity of the actual real-world users can be ascertained. The avatar has the legal authority in the virtual world to legally bind the user. This creates a chain of trust linking the avatar to the real-world user whose identity has been properly verified in accordance with law with a registration authority whose own status as a registration authority was verified at the time the user account was created. Users of the virtual world can thus interact with other avatars with a much enhanced sense of trust in reliance on the fact that the avatars are legal extensions of registered users whose identities have been properly verified by a registration authority having a legal capacity to verify the identities of persons within a given jurisdiction.

[00107] Verification of the RA and of users of the virtual world may be accomplished using the LB-SVS and the SVS. As depicted in FIG. 10, a status verification request is transmitted at step 1000 to a licensing body status verification server (LB-SVS) to ascertain that the RA is licensed to practice as an RA in that jurisdiction. A further status verification request is transmitted at step 1010 to the SVS to verify that the user is a registered user whose identity has been verified by an RA. Once these verifications have been performed, the RA may create a user

account at step 1020, thereby admitting the user as a member of the virtual world.

[00108] In one embodiment, the legal transaction management (LTM) application controls, manages and mediates all legal transactions within the virtual world. For example, if User A wishes to enter into a contract with User B (which is effectively e-commerce conducted in a virtual world via avatars), then the LTM application verifies that the users have real-world authority to enter into the contract. For example, the user may only be legally entitled to enter a contract if the user is of the age of majority. As another example, the user may only be entitled to transfer ownership to another user who fulfills certain criteria. The legal transaction management application thus polices certain actions to ensure that they are undertaken in accordance with the legal capacity of the users and in accordance with the authority conferred on the avatar by the user.

[00109] As depicted by way of example in FIG. 10, the LTM application enables commerce in a virtual world. The LTM may process a virtual contract between avatars according to a method as follows: at step 1030, the LTM application receives user input from a first user controlling a first avatar in the virtual world that causes the first avatar to present an offer to enter into a contract to a second avatar representing a second user, e.g. by communicating a electronic document representing the offered contract from the first avatar to the second avatar. This offer is presented in the virtual world. However, the offer may indirectly have a real-world effect, i.e. actual legal ramifications to the users, assuming there is a correlation between the value of currency (money) in the virtual world and the value of currency the real world. The LTM application then automatically verifies at step 1040 that the first user and the second user have legal authority to

enter into the contract. At step 1050, the LTM application then permits the second user to accept the offer to form a legally binding contract only if the first and second users have legal authority to contract. For example, the legal transaction management application may consider various factors and conditions in determining whether the avatars have the legal authority from their users to enter the contract. The factors and conditions may include the object of the contract, the age of each user, the residency of each user, the value of the transaction, restrictions imposed on the avatars by the virtual world, restrictions imposed on the avatars by the users, etc. The LTM application thus provides a system for avatars to engage in transactions that are meant to have direct or indirect legal effect in the real-world. The SVS furthermore acts as a gatekeeper or guardian of the virtual world, ensuring that only registered users whose identities have been verified by a registration authority are admitted to the virtual world. This creates a closed online community of trusted entities in which every avatar is linked to a single user such that the user cannot repudiate the acts of his avatar.

[00110] Any of the methods disclosed herein may be implemented in hardware, software, firmware or any combination thereof. Where implemented as software, the method steps, acts or operations may be programmed or coded as computer-readable instructions and recorded electronically, magnetically or optically on a non-transitory computer-readable medium, computer-readable memory, machine-readable memory or computer program product. In other words, the computer-readable memory or computer-readable medium comprises instructions in code which when loaded into a memory and executed on a processor of a computing device cause the computing device to perform one or more of the foregoing method(s).

[00111] A computer-readable medium can be any means that contain, store, communicate, propagate or transport the program for use by or in connection with the instruction execution system, apparatus or device. The computer-readable

5 medium may be electronic, magnetic, optical, electromagnetic, infrared or any semiconductor system or device. For example, computer executable code to perform the methods disclosed herein may be tangibly recorded on a computer-readable medium including, but not limited to, a floppy-disk, a CD-ROM, a DVD,
10 RAM, ROM, EPROM, Flash Memory or any suitable memory card, etc. The method may also be implemented in hardware. A hardware implementation might employ discrete logic circuits having logic gates for implementing logic functions on data signals, an application-specific integrated circuit (ASIC)
15 having appropriate combinational logic gates, a programmable gate array (PGA), a field programmable gate array (FPGA), etc.

[00112] This invention has been described in terms of specific embodiments, implementations and configurations which are intended to be exemplary only. Persons of ordinary skill in
20 the art will appreciate, having read this disclosure, that many obvious variations, modifications and refinements may be made without departing from the inventive concept(s) presented herein. The scope of the exclusive right sought by the Applicant(s) is therefore intended to be limited solely by the
25 appended claims.

CLAIMS:

1. A computer-implemented method of managing role-based digital rights in a computer system, the method comprising:

verifying a legal status of a first user seeking to act as a registration authority by sending a status verification request to a licensing body server that stores status information regarding the legal status of the first user to ascertain that the first user is licensed to act as the registration authority;

verifying a legal status of an organization having a hierarchical structure of roles by sending a status verification request to a status verification server that stores status information regarding the legal status of the organization verified by the registration authority or by any other registration authority deriving authority from an original registration authority;

if the legal statuses of the first user and the organization are verified, permitting user input from the registration authority to create an account for the organization within a document-interaction and transaction management application that enables interaction with electronic documents securely stored in a virtual vault and electronic transactions to be performed for the organization;

verifying a legal status of a first member of the organization by sending a status verification request to the status verification server, the first member having been verified by the registration authority or by any other registration authority deriving authority from the original registration authority, wherein the registration authority also verifies that the first member has a legal capacity to act in the first role; and

if the legal status of the first member is verified, permitting user input from the registration authority to define a first role within the organization for the first member, the first role conferring a first authority to act on behalf of the organization, wherein the first authority of the first member is predicated on the registration authority.

2. The method as claimed in claim 1 further comprising receiving user input from the first member to create a second role for a second member in compliance with internal governance

rules that are determined by legal requirements imposed on the organization, the second role conferring a second authority to act on behalf of the organization, thereby creating a chain of trust that predicates the second authority of the second role on the first authority of the first role which, in turn, is predicated on the status verification of the registration authority.

3. The method as claimed in claim 2 comprising:

receiving user input from the second member to perform a restricted action in the application;

verifying that the second member has requisite authority to perform the restricted action;
and

performing the restricted action in the application only if the second member has the requisite authority.

4. The method as claimed in claim 1 comprising assigning a plurality of first roles to a plurality of first members, the first members being governed by a reconfigurable majority-rule governance scheme.

5. A computer-readable medium comprising programmed instructions in code which, when loaded into a memory and executed by a processor of a computing device, causes the computing device to:

verify a legal status of a first user seeking to act as a registration authority by sending a status verification request to a licensing body server that stores status information regarding the legal status of the first user to ascertain that the first user is licensed to act as the registration authority;

verify a legal status of an organization having a hierarchical structure of roles by sending a status verification request to a status verification server that stores status information regarding the legal status of the organization verified by the registration authority or by any other registration authority deriving authority from an original registration authority;

if the legal statuses of the first user and the organization are verified, permit user input

from the registration authority to create an account for the organization within a document-interaction and transaction management application that enables interaction with electronic documents securely stored in a virtual vault and electronic transactions to be performed for the organization;

verify a legal status of a first member of the organization by sending a status verification request to the status verification server, the first member having been verified by the registration authority or by any other registration authority deriving authority from the original registration authority, wherein the registration authority also verifies that the first member has a legal capacity to act in the first role; and

if the legal status of the first member is verified, permit user input from the registration authority to define a first role within the organization for the first member, the first role conferring a first authority to act on behalf of the organization, wherein the first authority of the first member is predicated on the registration authority.

6. The computer-readable medium as claimed in claim 5 further comprising code to receive user input from the first member to create a second role for a second member in compliance with internal governance rules that are determined by legal requirements imposed on the organization, the second role conferring a second authority to act on behalf of the organization, thereby creating a chain of trust that predicates the second authority of the second role on the first authority of the first role which, in turn, is predicated on the status verification of the registration authority.

7. The computer-readable medium as claimed in claim 6 comprising code for:

receiving user input from the second member to perform a restricted action in the application;

verifying that the second member has requisite authority to perform the restricted action; and

performing the restricted action in the application only if the second member has the requisite authority.

8. The computer-readable medium as claimed in claim 5 comprising code for assigning a plurality of first roles to a plurality of first members, the first members being governed by a reconfigurable majority-rule governance scheme.

9. A computer system for managing role-based digital rights, the system comprising:

an application server having a processor operatively coupled to a memory to execute a document-interaction and transaction management application that enables interaction with electronic documents securely stored in a virtual vault and electronic transactions to be performed for the organization;

a licensing body server for verifying a legal status of a first user seeking to act as a registration authority by receiving a status verification request and for that stores status information regarding the legal status of the first user to ascertain that the first user is licensed to act as the registration authority;

a status verification server for storing status information about organizations and members whose legal status has been verified by the registration authority or any other registration authority deriving authority from an original registration authority, wherein the registration authority also verifies that the first member has a legal capacity to act in the first role;

wherein the application executing on the application server is programmed to:

send a status verification request to the licensing body server to verify the status of the registration authority;

send a status verification request to the status verification server to verify a status of an organization;

if the legal status of the first user and the organization are verified, permit user input from the registration authority to create an account for the organization within the application;

send a status verification request to the status verification server to verify a status of a first member of the organization; and

if the legal status of the first member is verified, permit user input to define a first role within the organization for the first member, the first role conferring a first authority to act on behalf of the organization, wherein the first authority of the first member is predicated on the registration authority.

10. The system as claimed in claim 9 wherein the application is programmed to receive user input from the first member to create a second role for a second member in compliance with internal governance rules that are determined by legal requirements imposed on the organization, the second role conferring a second authority to act on behalf of the organization, thereby creating a chain of trust that predicates the second authority of the second role on the first authority of the first role which, in turn, is predicated on the status verification of the registration authority.

11. The system as claimed in claim 10 wherein the application is programmed to:

receive user input from the second member to perform a restricted action in the application;

verify that the second member has requisite authority to perform the restricted action; and

perform the restricted action in the application only if the second member has the requisite authority.

12. The system as claimed in claim 9 wherein the application is programmed to assign a plurality of first roles to a plurality of first members, the first members being governed by a reconfigurable majority-rule governance scheme.

13. A computerized method of e-commerce between a first organization and a second organization each having a hierarchical structure of roles defined within a shared web-hosted document-interaction and transaction management application, wherein the roles confer different authorities to transact on behalf of the respective organizations, the method comprising:

verifying by the registration authority that a first member of the first organization has a legal capacity to act in a first role within the first organization;

if the legal capacity of the first member is verified, permitting the first member to define a role for an offering member;

verifying by the registration authority that a second member of the second organization has a legal capacity to act in a second role within the second organization;

if the legal capacity of the second member is verified, permitting the second member to define a role for an accepting member;

receiving user input from the offering member of the first organization requesting that the application generate an electronic contract document representing an offer to enter into a contract;

verifying by the application that the offering member of the first organization occupies a role having authority to contractually bind the first organization with respect to the contract;

generating the electronic contract document and permitting the first member to electronically sign the document only if the offering member has the authority to contractually bind the first organization with respect to the contract;

receiving user input identifying the accepting member who is to receive the electronic document at the second organization;

verifying by the application that the accepting member occupies a role conferring authority to accept the offer on behalf of the second organization;

transmitting the electronic contract document from the offering member of the first organization to the accepting member of the second organization if the accepting member has the authority to accept the offer;

receiving user input from the accepting member of the second organization by electronically signing the document to accept the offer; and

transmitting an electronic acceptance of the contract to the offering member of the first organization.

14. The method as claimed in claim 13 further comprising displaying a transaction dashboard presenting names and respective roles of all of the members that must electronically sign the document to be legally valid and further displaying a signature status indicating whether each member has signed the document.

15. The method as claimed in claim 13 further comprising sequentially notifying each of the members who must electronically sign the document in a predetermined order.

16. The method as claimed in claim 13 further comprising creating and sending a counteroffer to the first organization and determining if the offering member of the first organization still has authority to accept the counteroffer.

17. The method as claimed in claim 13 further comprising determining that the accepting member is non-responsive, determining whether the offer is time-limited, and automatically notifying another member whose role confers an equivalent authority to accept the offer.

18. A computer-readable medium comprising programmed instructions in code which, when loaded into a memory and executed by a processor of one or more computing devices, causes the one or more computing devices to execute a document-interaction and transaction management application for e-commerce between a first organization and a second organization each having a hierarchical structure of roles conferring different authorities to transact on behalf of the respective organizations, by:

verifying by the registration authority that a first member of the first organization has a legal capacity to act in a first role within the first organization;

if the legal capacity of the first member is verified, permitting the first member to define a role for an offering member;

verifying by the registration authority that a second member of the second organization has a legal capacity to act in a second role within the second organization;

if the legal capacity of the second member is verified, permitting the second member to define a role for an accepting member;

receiving user input from the offering member of the first organization requesting that the application generate an electronic contract document representing an offer to enter into a contract;

verifying by the application that the offering member of the first organization occupies a role having authority to contractually bind the first organization with respect to the contract;

generating the electronic contract document and permitting the first member to electronically sign the document only if the offering member has the authority to contractually bind the first organization with respect to the contract;

receiving user input identifying an accepting member who is to receive the electronic document at the second organization;

verifying by the application that the accepting member occupies a role conferring authority to accept the offer on behalf of the second organization;

transmitting the electronic contract document from the offering member of the first organization to the accepting member of the second organization if the accepting member has the authority to accept the offer;

receiving user input from the accepting member of the second organization by electronically signing the document to accept the offer; and

transmitting an electronic acceptance of the contract to the offering member of the first organization.

19. The computer-readable medium as claimed in claim 18 further comprising code for displaying a transaction dashboard presenting names and respective roles of all of the members that must electronically sign the document to be legally valid and further displaying a signature status indicating whether each member has signed the document.

20. The computer-readable medium as claimed in claim 18 further comprising code for sequentially notifying each of the members who must electronically sign the document in a predetermined order.

21. The computer-readable medium as claimed in claim 18 further comprising code for creating and sending a counteroffer to the first organization and determining if the offering member of the first organization still has authority to accept the counteroffer.

22. The computer-readable medium as claimed in claim 18 further comprising code for determining that the accepting member is non-responsive, determining whether the offer is time-limited, and automatically notifying another member whose role confers an equivalent authority to accept the offer.

23. A computer system for e-commerce, the system comprising:

an application server having a processor coupled to a memory for executing instructions in code of a document-interaction and transaction management application to facilitate e-commerce between a first organization and a second organization each having a hierarchical structure of roles conferring different authorities to transact on behalf of the respective organizations;

a status verification server in communication with the application server for verifying by the registration authority that a first member of the first organization has a legal capacity to act in a first role within the first organization and, if the legal capacity of the first member is verified, signalling to the application that the first member is authorized to define a role for an offering member;

the status verification also verifying by the registration authority that a second member of the second organization has a legal capacity to act in a second role within the second organization and, if the legal capacity of the second member is verified, signalling to the application that the second member is authorized to define a role for an accepting member;

a first computing device for receiving user input from the offering member of the first organization requesting that the application generate an electronic contract document representing an offer to enter into a contract;

the application verifying that the offering member of the first organization occupies a role having authority to contractually bind the first organization with respect to the contract;

the application generating the electronic contract document and permitting the offering member to electronically sign the document only if the offering member has the authority to contractually bind the first organization with respect to the contract;

the first computing device receiving user input identifying the accepting member who is to receive the electronic document at the second organization;

the application verifying that the accepting member occupies a role conferring authority to accept the offer on behalf of the second organization;

the application transmitting the electronic contract document from the offering member of the first organization to the accepting member of the second organization if the accepting member has the authority to accept the offer;

a second computing device for receiving user input from the accepting member of the second organization by electronically signing the document to accept the offer; and

the application transmitting an electronic acceptance of the contract to the offering member of the first organization.

24. The system as claimed in claim 23 wherein the second computing device displays a transaction dashboard presenting names and respective roles of all of the members that must electronically sign the document to be legally valid and further displaying a signature status indicating whether each member has signed the document.

25. The system as claimed in claim 23 wherein the second computing device sequentially notifies each of the members who must electronically sign the document in a predetermined order.

26. The system as claimed in claim 23 wherein the second computing device receives user input from the accepting member to create and send a counteroffer to the first organization and wherein the application determines if the offering member of the first organization still has authority to accept the counteroffer.

27. The system as claimed in claim 23 wherein the application comprises code for

determining that the accepting member is non-responsive, determining whether the offer is time-limited, and automatically notifying another member whose role confers an equivalent authority to accept the offer.

28. A computer-implemented method of managing role-based digital rights in a computer system, the method comprising:

verifying a legal status of a registration authority by sending a status verification request to a licensing body status verification system to ascertain that the registration authority is licensed to act as the registration authority;

verifying a legal status of an entity by sending a status verification request to an entity status verification system that stores status information regarding the legal status of the entity verified by the registration authority or by any other registration authority deriving authority from an original registration authority;

if the legal status of the entity is verified, permitting user input from the registration authority to create an account for the entity within a document-interaction and transaction management application that enables interaction with electronic documents securely stored in a virtual vault and electronic transactions to be performed for the entity;

verifying a legal status of a first member associated with the entity by sending a status verification request to the entity status verification system, the first member having been verified by the registration authority or by any other registration authority deriving authority from the original registration authority, wherein the registration authority also verifies that the first member has a legal capacity to act on behalf of the entity; and

if the legal status of the first member is verified, permitting user input from the registration authority to define a first role in relation to the entity for the first member, the first role conferring a first authority to act on behalf of the entity, wherein the first authority of the first member is predicated on the registration authority.

29. A computer-implemented method of conferring legal authority to avatars that represent users within a computer-generated virtual world in which the users interact with each other via

their respective avatars, the method comprising:

verifying a legal status of a registration authority by sending a status verification request to a licensing body status verification system to ascertain that the registration authority is licensed to act as the registration authority;

verifying a status and capacity of a user seeking to become a member of the virtual world by sending a status verification request to a status verification system that stores status information regarding the legal status of the user and the legal capacity to become a member of the virtual world, wherein the legal status and legal capacity have been verified by the registration authority or by any other registration authority deriving authority from an original registration authority; and

if the status of the user is verified, permitting user input from the registration authority to create an account for the member within the virtual world, the account linking the member to a unique avatar, wherein the authority of the avatar in the virtual world is predicated on the registration authority.

30. The method as claimed in claim 29 further comprising providing a legal transaction management application that enables legally binding interactions and transactions between avatars within the virtual world.

31. The method as claimed in claim 29 further comprising:

receiving user input from a first user controlling a first avatar in the virtual world that causes the first avatar to present an offer to enter into a contract to a second avatar representing a second user;

automatically verifying that the first user and the second user have legal authority to enter into the contract; and

permitting the second user to accept the offer to form a legally binding contract only if the first and second users have legal authority.