Non-Provisional Utility Patent Application Filing

Utility Patent Application Number: **19/096,071**
Filing Date: **31-MAR-2025**

WHAT'S NEXT?

1) **Filing Receipt From USPTO**
The US Patent Office will send a filing receipt in about 4-6 weeks. This comes in PDF format and when we receive it, we will email it to you. There is no need to wait for this document. The application is filed and *patent pending* as of the filing date above.
2) **Examination by USPTO**
The US Patent Office will examine your patent application and find inventions similar to yours, called prior art. If the examiner believes your invention is unique enough, the examiner may issue a notice of allowance at which time issuance fees will be due to formally grant the approved patent. If the examiner wants to discuss the similarities of your invention to other inventions the examiner has found, the examiner will issue a letter called an office action stating why the examiner thinks your invention is too similar to prior art. If this should happen, you have an opportunity to ask our attorneys to argue back for approval. On average, it may take 18-24 months before the US Patent Office examines your patent application. Hang tight, in the meantime, your invention is patent pending, and you can and should label your invention as such.

IMPORTANT DEADLINES:

1) **FILE INTERNATIONAL PATENT APPLICATIONS WITHIN 12 MONTHS**
A patent application in a foreign country can claim your US patent app filing date if filed within 12 months of the US filing. For example, you could file a patent application in Canada within 12 months and the Canada application can inherit the US patent application filing date. If you cannot file all the international patent applications you wish to file within 12 months, you can file a PCT application to extend the time to file international patent apps by an additional 18 months. You then have 18 additional months to file all international patent application which will claim the US application filing date. The key is that something must be done within 12 months. Either you file all the international patent applications you desire, or, you extend the time to file international patent applications by 18 months by filing a PCT. **In the next 12 months, if you don't file international patent applications and you don't file a PCT to extend the international filing window, you may lose the ability to apply for international patents**. Therefore, it is important to plan to file all international patent applications, or file a PCT, within the next 12 months. If you intend to file internationally, log your calendar to notify us at least 2 months before the 12 month period ends. We do not remind you of this deadline.

To learn more about the PCT application: https://www.thoughtstopaper.com/blog/what-is-a-pct-patent-application/

It is your responsibility to let us know you want to file internationally, well ahead of the deadlines.

If you missed the above deadline to file internationally, you may still be able to file in some countries, but not all. Each country's patent rules are different. Ask us to review your specific scenario and countries you wish to file in.

2) **<u>FILE DESIGN PATENT APPLICATIONS BEFORE YOU SHOW YOUR INVENTION TO THE PUBLIC</u>**
Your patent application covers the *utility* of your invention (how your invention works). However, it does not cover the *design* of your invention (how your invention looks). If you also want to prevent others from making an invention that looks like yours, you should also apply for a design patent. Design patent applications should be filed before you show your invention to the public. **<u>After your invention is shown to the public, you lose the ability to file design patent applications in many countries</u>**. It is important to note that this patent application we just filed will be published to the public by the US Patent Office in approximately 18 months. Therefore, even if you do not show your invention to the public yourself, the US Patent Office will eventually. Once the invention is shown to the public, you lose the ability to file design patent applications in many countries. Therefore, **you should request design patent applications in all countries you want design rights in as soon as possible**.

KEEP IN MIND:

1) **Let us know if your contact information changes**
As we represent you before the patent office, the patent office will send notices to us only and not directly to you. We then forward these notices to you by email. Most notices from the patent office have a strict due date for us to reply to. It is therefore important for you to update us if your email, mail, or phone number changes so that we can ensure delivery of important notifications to you. Further, it is important for you to regularly check your email and mail so as to not miss any notices which have a deadline.
2) **Let us know if you become aware of similar inventions invented before yours**
US patent law states that you as the inventor have the obligation to report to the patent office any inventions made before yours that you are aware of or even become aware of after you have filed your patent application. Failure to do so could result in loss of patent rights. If you become aware of such similar inventions, send them to us so that we can submit them to the US Patent Office. A fee will be required.
3) **Improvements to the invention can be filed as child applications**
Once a patent application is filed, no new information can be added to it. If you make an improvement to your invention that you wish to protect in a patent application, we need to do so by filing a second patent application to cover the new version, we call a child application. This should be done as soon as possible so that the improved version is also protected with a patent application.

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
19/096,071	**03/31/2025 05:10:56 PM Z ET**	**TUP89275**

Title of Invention

METHODS AND SYSTEMS FOR FACILITATING DECENTRALIZED MANAGEMENT OF A KNOWLEDGE GRAPH

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	7782	FILED BY	HEATHER BOOKHULTZ
PATENT CENTER #	69811480	FILING DATE	-
CUSTOMER #	62439	FIRST NAMED INVENTOR	Richard Gillespie
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	COLBY MACIAS

Documents

TOTAL DOCUMENTS: 10

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
ADS_TUP89275.pdf	8	Application Data Sheet	2173 KB
Drawings_TUP89275_emb.pdf	22	Drawings-only black and white line drawings	137 KB
Specs_TUP89275-APP.TEXT.docx	52	Application body structured text document	58 KB
NPL1.pdf	3	Non Patent Literature	194 KB
NPL3.pdf	5	Non Patent Literature	871 KB
NPL2.pdf	26	Non Patent Literature	1638 KB
pto15_TUP89275.pdf	1	Certification of Micro Entity (Gross Income Basis)	1670 KB

poa_TUP89275.pdf	2	Power of Attorney	3659 KB
Dec_TUP89275.pdf	2	Oath or Declaration filed	2163 KB
IDS SB-08a 01-25.pdf	5	Information Disclosure Statement (IDS) Form (SB08)	1315 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
ADS_TUP89275.pdf	FCD52A5EF8DE1E777D49BF5B09A9C8DD978D6CC4DAD5F5805D7A1D99DC205F2AEC2707FC5B27EFDF9669FD0F4074202579DBA173BF6C04551622D37D6630ED0A
Drawings_TUP89275_emb.pdf	1604816A166B341B1724C9FAD3C2B5FB3B9B233CECE7ACEE9063A975AB91FE70EA5A2ECDDC0849FAEBC378EDE2BBD3F656ABC5C575E160473306023FD2ABEE27
Specs_TUP89275-APP.TEXT.docx	6C8A4D72FF2FC7C1E018F83B8AEBA1CCD8406892C1DC91C505BDF9336DB589BB16BB932F69468AAA77D4D323B049A6EBBB511ACE7ACBB044716FCCB5D9C4EF3D
NPL1.pdf	95CF3F77543B420E9D42DFEC9C58683AE0227D33E99B1893BB8AAFBCC00924C137D1D4B8D719E3D972FB60F62EE136C3A64A6F4232C59A3AD2C5376B7B68CCFD
NPL3.pdf	EA921AC0A58CA04ABEAC08F99F6D09E40507D7BF5577C1C0474E5F0B9D2684867EEA0161BD978D741AF142F62C0E4A1B9CBA4DB193B1783ED3CAB1D3795C98EE
NPL2.pdf	FB321160437B07DDCF833DF0E47B12F794C5025CAF1440B3076342C560AD07833D6A381D7C20AC08511CE33062941B4B73164B82080B24528E7C3FCF70DD4720
pto15_TUP89275.pdf	6A57D53FC8EC0C61790D8A1CCC82FE1C7D63153F26E75DBCB9B86F40DABA99ABB535E83E18F5B6D567072C9F956C171D573DD293015F05593EF2629D4E9179B4
poa_TUP89275.pdf	844546976D1A3CA7BC9B9C66C128EDFCFFC8CF07F528032CE22F6E26477562D3FCBDAD1BD3B71DA1A7AB82153A77FAB4DCA4A192B2E802EF1E1E214B31745B22
Dec_TUP89275.pdf	5206EB055F1FBA303D6A6D5384988B4B8D80F3330D5305CC81BD729F3354F74CEF4853BC37FE5BA553CD19C78162C0BE291497BCBE2FD2C6DE93585A8AB9371F
IDS SB-08a 01-25.pdf	1D14FF3509FCAE4434ADA8BEC4AD1C300614F509E51ADBE56954190FC3E76B5A8594465DFE8784F04AD45889A548EBE6D9D09FC35CE474C9B70FD8E9BC2CF426

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

METHODS AND SYSTEMS FOR FACILITATING DECENTRALIZED MANAGEMENT OF A KNOWLEDGE GRAPH

FIELD OF DISCLOSURE

The present disclosure generally relates to a field of data processing. More specifically, the present disclosure relates to methods and systems for facilitating decentralized management of a knowledge graph.

BACKGROUND

The field of knowledge graph management has become increasingly important in recent years as organizations seek to integrate, organize, and utilize vast amounts of data across diverse domains. Knowledge graphs, which represent structured and interconnected information, are critical for enabling semantic search, decision-making, and intelligent applications. These systems are utilized in various industries, including finance, healthcare, education, and technology, to manage complex relationships between entities, such as people, places, concepts, and events.

Existing knowledge graph management systems face significant challenges. One primary issue is the lack of robust mechanisms for ensuring data integrity and authenticity. Without reliable methods for validating changes or transactions, organizations risk suffering data breaches, fraud, or misinterpretation of information. Additionally, traditional approaches to knowledge graph management often lack transparency, making it difficult to trace the origin or history of data updates, which can lead to accountability issues.

Another critical challenge is the need for efficient and ethical governance of knowledge graphs. As knowledge graphs grow in size and complexity, managing ethical standards, transformation parameters, and domain-specific guidelines becomes increasingly complex. Existing systems often lack mechanisms for real-time

collaboration among domain experts, leading to delays, inconsistencies, or poorly informed decisions.

Further, the existing systems lack mechanisms for storing knowledge graph in a verifiable and human-readable format, dynamically generating transformation agents based on real-time training data and adaptive audit feedback, validating candidate output against ethical and moral standards via foundational ethics node, recording every transaction on an immutable block-chain sidechain and enabling decentralized governance for real-time collaborative update.

Moreover, the scalability and monetization of knowledge graph access pose additional challenges. Many knowledge graph platforms struggle with balancing accessibility with security, often requiring costly subscriptions or licenses that limit adoption. Additionally, traditional licensing models may not align with the dynamic nature of knowledge graphs, where usage patterns can vary significantly over time.

Therefore, there is a need for improved methods and systems for facilitating a decentralized management of a knowledge graph, that may overcome one or more of the above-mentioned problems and/or limitations.

SUMMARY OF DISCLOSURE

This summary is provided to introduce a selection of concepts in a simplified form, that are further described below in the Detailed Description. This summary is not intended to identify key features or essential features of the claimed subject matter. Nor is this summary intended to be used to limit the claimed subject matter’s scope.

The present disclosure provides a method for facilitating decentralized management of a knowledge graph. Further, the method may include receiving, using a communication device, a domain data from a user device associated with a user. Further, the domain data corresponds to a subject matter within a domain. Further, the method

may include analyzing, using a processing device, the domain data. Further, the method may include generating, using the processing device, a knowledge graph operation data based on the analyzing. Further, the knowledge graph operation data includes one or more of a creation data which may be configured for creating a knowledge graph data and an updation data which may be configured for updating the knowledge graph data. Further, the method may include executing, using the processing device, one or more of the creating and the updating. Further, the method may include storing, using a storage device, the knowledge graph operation data on a decentralized database.

The present disclosure provides a system for facilitating decentralized management of a knowledge graph. Further, the system may include a communication device. Further, the communication device may be configured for receiving a domain data from a user device associated with a user. Further, the domain data corresponds to a subject matter within a domain. Further, the system may include a processing device communicatively coupled with the communication device. Further, the processing device may be configured for analyzing the domain data. Further, the processing device may be configured for generating a knowledge graph operation data based on the analyzing. Further, the knowledge graph operation data includes one or more of a creation data which may be configured for creating a knowledge graph data and an updation data which may be configured for updating the knowledge graph data. Further, the processing device may be configured for executing one or more of the creating and the updating. Further, the system may include a storage device which may be configured for storing the knowledge graph operation data on a decentralized database.

Both the foregoing summary and the following detailed description provide examples and are explanatory only. Accordingly, the foregoing summary and the following detailed description should not be considered to be restrictive. Further, features or variations may be provided in addition to those set forth herein. For example, embodiments may be directed to various feature combinations and sub-combinations described in the detailed description.

BRIEF DESCRIPTIONS OF DRAWINGS

The accompanying drawings, which are incorporated in and constitute a part of this disclosure, illustrate various embodiments of the present disclosure. The drawings contain representations of various trademarks and copyrights owned by the Applicants. In addition, the drawings may contain other marks owned by third parties and are being used for illustrative purposes only. All rights to various trademarks and copyrights represented herein, except those belonging to their respective owners, are vested in and the property of the applicants. The applicants retain and reserve all rights in their trademarks and copyrights included herein, and grant permission to reproduce the material only in connection with reproduction of the granted patent and for no other purpose.

Furthermore, the drawings may contain text or captions that may explain certain embodiments of the present disclosure. This text is included for illustrative, non-limiting, explanatory purposes of certain embodiments detailed in the present disclosure.

Fig. 1 is an illustration of an online platform 100 consistent with various embodiments of the present disclosure.

Fig. 2 is a block diagram of a computing device 200 for implementing the methods disclosed herein, in accordance with some embodiments.

Fig. 3 illustrates a flowchart of a method 300 for facilitating decentralized management of a knowledge graph, in accordance with some embodiments.

Fig. 4 illustrates a flowchart of a method 400 for facilitating decentralized management of a knowledge graph including generating, using the processing device 1204, a response data, in accordance with some embodiments.

Fig. 5 illustrates a flowchart of a method 500 for facilitating decentralized management of a knowledge graph including retraining, using the processing device 1204, the transformation agent, in accordance with some embodiments.

Fig. 6 illustrates a flowchart of a method 600 for facilitating decentralized management of a knowledge graph including retraining, using the processing device 1204, the transformation agent, in accordance with some embodiments.

Fig. 7 illustrates a flowchart of a method 700 for facilitating decentralized management of a knowledge graph including retraining, using the processing device 1204, the transformation agent, in accordance with some embodiments.

Fig. 8 illustrates a flowchart of a method 800 for facilitating decentralized management of a knowledge graph including analyzing, using the processing device 1204, the validation data, in accordance with some embodiments.

Fig. 9 illustrates a flowchart of a method 900 for facilitating decentralized management of a knowledge graph including generating, using the processing device 1204, an agent data, in accordance with some embodiments.

Fig. 10 illustrates a flowchart of a method 1000 for facilitating decentralized management of a knowledge graph including generating, using the processing device 1204, a reward data, in accordance with some embodiments.

Fig. 11 illustrates a flowchart of a method 1100 for facilitating decentralized management of a knowledge graph including generating, using the processing device 1204, a signature data, in accordance with some embodiments.

Fig. 12 illustrates a block diagram of a system 1200 for facilitating decentralized management of a knowledge graph, in accordance with some embodiments.

Fig. 13 illustrates a flowchart of a method 1300 for facilitating decentralized management of a knowledge graph including generating, using the processing device 1204, a time data, in accordance with some embodiments.

Fig. 14 illustrates a flowchart of a method 1400 for facilitating decentralized management of a knowledge graph including generating, using the processing device 1204, a configuration data, in accordance with some embodiments.

Fig. 15 illustrates a flowchart of a method 1500 for facilitating decentralized management of a knowledge graph including generating, using the processing device 1204, a cost data, in accordance with some embodiments.

Fig. 16 illustrates a flowchart of a method 1600 for facilitating decentralized management of a knowledge graph including generating, using the processing device 1204, an access token data, in accordance with some embodiments.

Fig. 17 illustrates a flowchart of a method 1700 for facilitating decentralized management of a knowledge graph including analyzing, using the processing device 1204, the access token data, in accordance with some embodiments.

Fig. 18 illustrates a flowchart of a method 1800 for facilitating decentralized management of a knowledge graph including retrieving, using the processing device 1204, the transformation agent from a plurality of transformation agents, in accordance with some embodiments.

Fig. 19 illustrates a flowchart of a method 1900 for facilitating decentralized management of a knowledge graph including training, using the processing device 1204, the transformation agent, in accordance with some embodiments.

Fig. 20 illustrates a system architecture, in accordance with some embodiments.

Fig. 21 illustrates a flowchart of decentralized management of a knowledge graph, in accordance with some embodiments.

Fig. 22 illustrates a top node schematic of decentralized management of a knowledge graph, in accordance with some embodiments.

DETAILED DESCRIPTION OF DISCLOSURE

As a preliminary matter, it will readily be understood by one having ordinary skill in the relevant art that the present disclosure has broad utility and application. As should be

understood, any embodiment may incorporate only one or a plurality of the above-disclosed aspects of the disclosure and may further incorporate only one or a plurality of the above-disclosed features. Furthermore, any embodiment discussed and identified as being "preferred" is considered to be part of a best mode contemplated for carrying out the embodiments of the present disclosure. Other embodiments also may be discussed for additional illustrative purposes in providing a full and enabling disclosure. Moreover, many embodiments, such as adaptations, variations, modifications, and equivalent arrangements, will be implicitly disclosed by the embodiments described herein and fall within the scope of the present disclosure.

Accordingly, while embodiments are described herein in detail in relation to one or more embodiments, it is to be understood that this disclosure is illustrative and exemplary of the present disclosure, and are made merely for the purposes of providing a full and enabling disclosure. The detailed disclosure herein of one or more embodiments is not intended, nor is to be construed, to limit the scope of patent protection afforded in any claim of a patent issuing here from, which scope is to be defined by the claims and the equivalents thereof. It is not intended that the scope of patent protection be defined by reading into any claim limitation found herein and/or issuing here from that does not explicitly appear in the claim itself.

Thus, for example, any sequence(s) and/or temporal order of steps of various processes or methods that are described herein are illustrative and not restrictive. Accordingly, it should be understood that, although steps of various processes or methods may be shown and described as being in a sequence or temporal order, the steps of any such processes or methods are not limited to being carried out in any particular sequence or order, absent an indication otherwise. Indeed, the steps in such processes or methods generally may be carried out in various different sequences and orders while still falling within the scope of the present disclosure. Accordingly, it is intended that the scope of patent protection is to be defined by the issued claim(s) rather than the description set forth herein.

Additionally, it is important to note that each term used herein refers to that which an ordinary artisan would understand such term to mean based on the contextual use of such

term herein. To the extent that the meaning of a term used herein—as understood by the ordinary artisan based on the contextual use of such term—differs in any way from any particular dictionary definition of such term, it is intended that the meaning of the term as understood by the ordinary artisan should prevail.

Furthermore, it is important to note that, as used herein, "a" and "an" each generally denotes "at least one," but does not exclude a plurality unless the contextual use dictates otherwise. When used herein to join a list of items, "or" denotes "at least one of the items," but does not exclude a plurality of items of the list. Finally, when used herein to join a list of items, "and" denotes "all of the items of the list."

The following detailed description refers to the accompanying drawings. Wherever possible, the same reference numbers are used in the drawings and the following description to refer to the same or similar elements. While many embodiments of the disclosure may be described, modifications, adaptations, and other implementations are possible. For example, substitutions, additions, or modifications may be made to the elements illustrated in the drawings, and the methods described herein may be modified by substituting, reordering, or adding stages to the disclosed methods. Accordingly, the following detailed description does not limit the disclosure. Instead, the proper scope of the disclosure is defined by the claims found herein and/or issuing here from. The present disclosure contains headers. It should be understood that these headers are used as references and are not to be construed as limiting upon the subjected matter disclosed under the header.

The present disclosure includes many aspects and features. Moreover, while many aspects and features relate to, and are described in the context of the disclosed use cases, embodiments of the present disclosure are not limited to use only in this context.

In general, the method disclosed herein may be performed by one or more computing devices. For example, in some embodiments, the method may be performed by a server computer in communication with one or more client devices over a communication network such as, for example, the Internet. In some other embodiments, the method may be performed by one or more of at least one server computer, at least one client device, at

least one network device, at least one sensor and at least one actuator. Examples of the one or more client devices and/or the server computer may include, a desktop computer, a laptop computer, a tablet computer, a personal digital assistant, a portable electronic device, a wearable computer, a smart phone, an Internet of Things (IoT) device, a smart electrical appliance, a video game console, a rack server, a super-computer, a mainframe computer, mini-computer, micro-computer, a storage server, an application server (e.g. a mail server, a web server, a real-time communication server, an FTP server, a virtual server, a proxy server, a DNS server etc.), a quantum computer, and so on. Further, one or more client devices and/or the server computer may be configured for executing a software application such as, for example, but not limited to, an operating system (e.g. Windows, Mac OS, Unix, Linux, Android, etc.) in order to provide a user interface (e.g. GUI, touch-screen based interface, voice based interface, gesture based interface etc.) for use by the one or more users and/or a network interface for communicating with other devices over a communication network. Accordingly, the server computer may include a processing device configured for performing data processing tasks such as, for example, but not limited to, analyzing, identifying, determining, generating, transforming, calculating, computing, compressing, decompressing, encrypting, decrypting, scrambling, splitting, merging, interpolating, extrapolating, redacting, anonymizing, encoding and decoding. Further, the server computer may include a communication device configured for communicating with one or more external devices. The one or more external devices may include, for example, but are not limited to, a client device, a third party database, public database, a private database and so on. Further, the communication device may be configured for communicating with the one or more external devices over one or more communication channels. Further, the one or more communication channels may include a wireless communication channel and/or a wired communication channel. Accordingly, the communication device may be configured for performing one or more of transmitting and receiving of information in electronic form. Further, the server computer may include a storage device configured for performing data storage and/or data retrieval operations. In general, the storage device may be configured for providing reliable storage of digital information. Accordingly, in some embodiments, the storage device may be based on

technologies such as, but not limited to, data compression, data backup, data redundancy, deduplication, error correction, data finger-printing, role based access control, and so on.

Further, one or more steps of the method disclosed herein may be initiated, maintained, controlled and/or terminated based on a control input received from one or more devices operated by one or more users such as, for example, but not limited to, an end user, an admin, a service provider, a service consumer, an agent, a broker and a representative thereof. Further, the user as defined herein may refer to a human, an animal or an artificially intelligent being in any state of existence, unless stated otherwise, elsewhere in the present disclosure. Further, in some embodiments, the one or more users may be required to successfully perform authentication in order for the control input to be effective. In general, a user of the one or more users may perform authentication based on the possession of a secret human readable secret data (e.g. username, password, passphrase, PIN, secret question, secret answer etc.) and/or possession of a machine readable secret data (e.g. encryption key, decryption key, bar codes, etc.) and/or or possession of one or more embodied characteristics unique to the user (e.g. biometric variables such as, but not limited to, fingerprint, palm-print, voice characteristics, behavioral characteristics, facial features, iris pattern, heart rate variability, evoked potentials, brain waves, and so on) and/or possession of a unique device (e.g. a device with a unique physical and/or chemical and/or biological characteristic, a hardware device with a unique serial number, a network device with a unique IP/MAC address, a telephone with a unique phone number, a smartcard with an authentication token stored thereupon, etc.). Accordingly, the one or more steps of the method may include communicating (e.g. transmitting and/or receiving) with one or more sensor devices and/or one or more actuators in order to perform authentication. For example, the one or more steps may include receiving, using the communication device, the secret human readable data from an input device such as, for example, a keyboard, a keypad, a touch-screen, a microphone, a camera and so on. Likewise, the one or more steps may include receiving, using the communication device, the one or more embodied characteristics from one or more biometric sensors.

Further, one or more steps of the method may be automatically initiated, maintained and/or terminated based on one or more predefined conditions. In an instance, the one or more predefined conditions may be based on one or more contextual variables. In general, the one or more contextual variables may represent a condition relevant to the performance of the one or more steps of the method. The one or more contextual variables may include, for example, but are not limited to, location, time, identity of a user associated with a device (e.g. the server computer, a client device etc.) corresponding to the performance of the one or more steps, environmental variables (e.g. temperature, humidity, pressure, wind speed, lighting, sound, etc.) associated with a device corresponding to the performance of the one or more steps, physical state and/or physiological state and/or psychological state of the user, physical state (e.g. motion, direction of motion, orientation, speed, velocity, acceleration, trajectory, etc.) of the device corresponding to the performance of the one or more steps and/or semantic content of data associated with the one or more users. Accordingly, the one or more steps may include communicating with one or more sensors and/or one or more actuators associated with the one or more contextual variables. For example, the one or more sensors may include, but are not limited to, a timing device (e.g. a real-time clock), a location sensor (e.g. a GPS receiver, a GLONASS receiver, an indoor location sensor etc.), a biometric sensor (e.g. a fingerprint sensor), an environmental variable sensor (e.g. temperature sensor, humidity sensor, pressure sensor, etc.) and a device state sensor (e.g. a power sensor, a voltage/current sensor, a switch-state sensor, a usage sensor, etc. associated with the device corresponding to performance of the or more steps).

Further, the one or more steps of the method may be performed one or more number of times. Additionally, the one or more steps may be performed in any order other than as exemplarily disclosed herein, unless explicitly stated otherwise, elsewhere in the present disclosure. Further, two or more steps of the one or more steps may, in some embodiments, be simultaneously performed, at least in part. Further, in some embodiments, there may be one or more time gaps between performance of any two steps of the one or more steps.

Further, in some embodiments, the one or more predefined conditions may be specified by the one or more users. Accordingly, the one or more steps may include receiving, using the communication device, the one or more predefined conditions from one or more and devices operated by the one or more users. Further, the one or more predefined conditions may be stored in the storage device. Alternatively, and/or additionally, in some embodiments, the one or more predefined conditions may be automatically determined, using the processing device, based on historical data corresponding to performance of the one or more steps. For example, the historical data may be collected, using the storage device, from a plurality of instances of performance of the method. Such historical data may include performance actions (e.g. initiating, maintaining, interrupting, terminating, etc.) of the one or more steps and/or the one or more contextual variables associated therewith. Further, machine learning may be performed on the historical data in order to determine the one or more predefined conditions. For instance, machine learning on the historical data may determine a correlation between one or more contextual variables and performance of the one or more steps of the method. Accordingly, the one or more predefined conditions may be generated, using the processing device, based on the correlation.

Further, one or more steps of the method may be performed at one or more spatial locations. For instance, the method may be performed by a plurality of devices interconnected through a communication network. Accordingly, in an example, one or more steps of the method may be performed by a server computer. Similarly, one or more steps of the method may be performed by a client computer. Likewise, one or more steps of the method may be performed by an intermediate entity such as, for example, a proxy server. For instance, one or more steps of the method may be performed in a distributed fashion across the plurality of devices in order to meet one or more objectives. For example, one objective may be to provide load balancing between two or more devices. Another objective may be to restrict a location of one or more of an input data, an output data and any intermediate data there between corresponding to one or more steps of the method. For example, in a client-server environment, sensitive data corresponding to a user may not be allowed to be transmitted to the server computer. Accordingly, one or

more steps of the method operating on the sensitive data and/or a derivative thereof may be performed at the client device.

Overview:

The present disclosure describes a decentralized, block-chain audited knowledge graph ecosystem with dynamic agent generation, adaptive token-based licensing, and foundational ethics self-validation for safe AI and multi-domain applications.

Further, the present disclosure describes a system and method for secure, decentralized management of knowledge graphs (KGs). The system and method integrates block-chain audited digital signatures, dynamic token-based licensing, decentralized governance, and an adaptive foundational ethics module to create human-readable, auditable, and self-evolving KGs. Further, the key feature includes a dynamic agent generation framework, wherein transformation agents whose executable code is stored within the KG are dynamically loaded, refined, and combined in real time to generate candidate solutions for abstract puzzles, complex mathematical problems, and ethical language games.

Further, candidate outputs are evaluated by a foundational ethics node that employs Aristotelian logic, Socratic dialectic inquiry, and Wittgensteinian language games to ensure ethical compliance. All transactions, transformation events, and governance actions are cryptographically hashed and recorded on a block-chain sidechain, providing transparent, immutable audit trails. Also, complex challenges found in abstract puzzles, mathematical proofs, and ethical dilemmas demand multifaceted, dynamic processing.

Further, an integrated language model backup supplies fallback solutions and natural language explanations, thereby safeguarding against rogue AI. The system establishes a monetizable, continuously adaptive framework applicable to diverse, high-risk domains.

The following are the components of the system and method for managing knowledge graph:

1. Blockchain-Audited Data Integrity and Dynamic Licensing:

Every update to the KG is digitally signed, timestamped, and aggregated using secure algorithms (e.g., SHA-256). The resulting hash is recorded on a block-chain sidechain, ensuring immutable, publicly verifiable audit trails. Token costs are dynamically computed based on real-time usage and transformation complexity, and smart contracts automatically process microtransactions to provide transparent, scalable revenue sharing.

2. Dynamic Transformation Agent Generation:
Transformation agents are stored as executable code (e.g., Groovy scripts) along with configuration data and performance metrics. Further, the transformation agents are dynamically retrieved, compiled, and instantiated by a Dynamic Agent Manager using a secure scripting engine. Adaptive learning driven by audit feedback and performance metrics continuously refines these agents and generates new combinations to address complex challenges.
3. Foundational Ethics Self-Validation:
A central ethics node, constructed at system initialization, aggregates ethical concepts, moral dilemmas, logical fallacies, and sample arguments. Employing Aristotelian logic, Socratic dialectic inquiry, and Wittgensteinian language games (which abstract the notion of shared internal dialogue), the ethics node evaluates candidate outputs. Further, outputs conforming to ethical standards are auto-approved; those posing significant ethical concerns are flagged for further adaptive refinement and expert review.
4. Decentralized Governance and Adaptive Learning:
Domain experts participate in a distributed voting process to update ethical standards and transformation parameters in real time. Governance events, together with performance and audit data, are recorded on the block-chain. This continuous feedback loop drives adaptive learning, ensuring the system evolves based on real-world performance and ethical evaluations.
5. Hybrid Integration with LLM Backup and Interoperability:
An integrated language model backup provides fallback solutions and natural language interpretations, converting plain language queries into actionable Cypher commands. The system is engineered for seamless interoperability with

external APIs and enterprise architectures, ensuring long-term scalability and adaptability.

Detailed Description:

1. System Architecture:

The system is implemented as a Neo4j plugin with fully Java- and Groovy-based components, comprising the following modules:

- Knowledge Graph Database (KG):
  The KG stores domain-specific data as human-readable nodes and relationships. Each update is digitally signed and timestamped; transactions are aggregated and hashed.
- Digital Signature and Blockchain Module:
  A Digital Signature Util signs data using RSA. A Transaction Aggregator and Hash Calculator compute secure SHA-256 hashes, which are recorded on a block-chain sidechain via Blockchain Connector and Smart Contract Handler (using an Ethereum-compatible network and web3j), ensuring tamper-proof audit trails. Further, uses PKI (such as RSA or ECC) to generate digital signatures for each KG transaction, ensuring data integrity and accountability.
- Dynamic Licensing Module:
  A Token Pricing Engine dynamically computes token costs based on real-time usage and transformation complexity. Revenue Sharing Manager and Licensing Procedures expose these metrics and process microtransactions via smart contracts, enabling equitable revenue sharing. It integrates with smart contracts, to automatically manage token transfers for both awarding tokens to domain experts and deducting tokens from users accessing the knowledge graphs.
- Foundational Ethics Node and Self-Validation:
  Built at initialization, the Ethics Node comprises nodes for Ethical Concepts, Moral Dilemmas, Logical Fallacies, and sample Arguments. An Ethics Validator evaluates candidate outputs from transformation agents against these standards using a multi-agent framework that combines

Aristotelian logic, Socratic dialectic inquiry, and Wittgensteinian language games. Adaptive learning mechanisms refine the evaluation process based on audit feedback.

- Adaptive Transformation Agent Engine:
  Transformation agent definitions including executable Groovy code, configuration data, and performance metrics are stored in the KG. The Dynamic Agent Manager retrieves, compiles, and instantiates these agents via a secure scripting engine. Further, the continuous monitoring of performance and audit logs drives adaptive learning, resulting in the dynamic generation and refinement of agent combinations.
- Learning Module and LLM Backup:
  The Learning KG Manager builds foundational KGs (such as an ARC Puzzle KG and a Math KG) at startup. Puzzle Solver ingests puzzles from training and evaluation datasets and logs performance outcomes for continuous adaptation. Conversational Agent and LLM Backup Client provide fallback natural language explanations and convert plain language queries into Cypher commands.
- Decentralized Governance:
  Governance Procedures and Vote Manager implement a distributed voting process that allows domain experts to update ethical standards and transformation parameters. All governance actions are recorded on the block-chain, ensuring transparency and accountability. Further, the voting mechanism allows the domain experts to validate, curate, and update their published knowledge graphs, thereby maintaining human oversight
- Interoperability and Extensibility:
  The system is designed to integrate seamlessly with external APIs, data formats, and enterprise software, ensuring that the ecosystem remains scalable and adaptable to future technological advances.
- Blockchain-Enabled Microtransactions:
  Each KG update, transformation event, and governance action triggers smart contract interactions that process dynamic token-based licensing and

revenue sharing. This monetizable framework incentivizes innovation and ensures that every interaction is securely logged.

Further, the system aggregates KG transactions over defined periods, computes a cryptographic hash, and synchronizes this hash with a block-chain sidechain to create an immutable audit record.

- Secure Authentication System:
  Implements multi-factor authentication (e.g., OAuth 2.0) and links user identities to block-chain wallets to ensure secure token transactions and access control.
- Training and Instructional Platform:
  An integrated training system that enhances the ARC Language Game inner dialog schema. This system allows domain experts to learn how to create and support their domain-specific KGs, ensuring that they can build, evolve, and monetize their own knowledge assets.

2. Workflow:
   - Initialization:
     The system initializes by executing the Main Plugin, which registers all custom procedures, builds foundational KGs, and deploys smart contracts for dynamic licensing at minimal fees. The Dynamic Agent Manager retrieves transformation agent definitions from the KG and instantiates them.
   - Puzzle Ingestion and Processing:
     Puzzles are ingested from training and evaluation datasets. The Dynamic Agent Manager applies transformation agents to generate candidate solutions, which are validated against the foundational Ethics Node. Non-compliant outputs trigger adaptive refinement through audit feedback and decentralized governance.
   - Ethical Validation and Adaptive Learning:
     The Ethics Validator reviews candidate outputs using a multi-agent reasoning framework. Adaptive Ethics Learning Agent updates internal parameters based on continuous audit feedback. Domain experts

participate in decentralized governance to vote on necessary changes, with all governance events recorded on the block-chain.

- User Interaction and Hybrid Integration:
  End users and domain experts interact with the system via Cypher queries or natural language interfaces. The integrated LLM backup provides fallback solutions and human-readable chain-of-thought explanations.
- Continuous Improvement:
  Performance metrics, audit logs, and governance events feed into a continuous improvement loop, allowing the dynamic update of transformation agents, ethical evaluation criteria, and licensing models.

3. Key Aspects:
   1. A method for secure, decentralized management of knowledge graphs, comprising:
      - Storing data in a human-readable KG with digital signatures and block-chain backed immutable audit trails;
      - Dynamically generating transformation agents based on real-time training data and adaptive audit feedback; and
      - Enforcing dynamic token-based licensing via smart contracts.
      - Further, the transformation agents are stored as executable code in the KG and are dynamically retrieved, compiled, and instantiated by a Dynamic Agent Manager using a secure scripting engine, with continuous refinement driven by performance metrics and audit logs.
      - Further, the method includes a foundational ethics node that evaluates candidate outputs using Aristotelian logic, Socratic dialectic inquiry, and language game abstractions, automatically approving compliant outputs and flagging non-compliant outputs for expert review.
      - Further, the method includes a decentralized governance process wherein domain experts collaboratively update ethical standards and transformation parameters via a distributed voting mechanism recorded on a block-chain.

- Further, the method integrates with a fallback language model to provide natural language explanations and convert plain language queries into actionable Cypher commands.
- Further, the method performs dynamic token-based licensing, wherein token costs are computed based on real-time usage metrics and transformation complexity, and microtransactions are processed via smart contracts.
- Further, the computer-readable storage medium containing instructions which, when executed by a processor, perform at least one of the above mentioned process.

2. A method for validating and monetizing domain-specific knowledge graphs, comprising:
    - Creating a foundational Ethics Node that stores ethical principles, moral dilemmas, and sample arguments;
    - Generating candidate outputs via multiple transformation agents and dynamically combining them to optimize solution accuracy;
    - Validating outputs against ethical standards and recording all validation events on a block-chain sidechain for immutable auditability; and
    - Enforcing dynamic token-based licensing for access to the learning module via smart contracts.
    - Further, the domain experts participate in a decentralized governance process to update ethical standards and system parameters, with all governance events recorded on the block-chain.
3. A method for incentivizing continuous learning in knowledge graph management, comprising:
    - Ingesting data from training and evaluation datasets;
    - Processing data using dynamically generated transformation agents;
    - Logging performance outcomes and audit feedback in the KG;
    - Automatically refining and generating new transformation agents based on logged performance data; and

- Distributing revenue through dynamic token-based licensing via smart contracts.

4. A method for safeguarding against rogue AI by integrating a foundational Ethics Node that continuously validates all outputs generated by dynamic transformation agents and enforces a decentralized governance process for real-time ethical oversight.

The system may offer a transparent, auditable, and continuously evolving solution for diverse, high-risk domains.

Further, the system is designed to empower domain experts to create, maintain, and monetize their own domain-specific knowledge graphs (KGs). It combines several advanced technologies to offer a decentralized ecosystem where:

- Domain experts (or "authors") use an AI-assisted process (abstractly represented as an "AI puzzle solving" mechanism) to generate and refine their knowledge graphs.
- Each interaction with the knowledge graph is secured through digital signatures, ensuring authenticity and traceability.
- The system periodically aggregates and commits cryptographic hashes of these transactions to a block-chain sidechain, creating an immutable, tamper-proof audit trail.
- Access to these published knowledge graphs is regulated through a dynamic token-based licensing mechanism; users pay tokens to access the data, and the tokens are automatically redistributed to the contributing experts.
- A decentralized governance framework enables continuous human oversight, ensuring that the technology remains safe and AI is used as a supportive, human-centric tool rather than an autonomous decision-maker.

The system operates by integrating multiple layers of technology into a unified ecosystem:

1. Digital Signing and Data Integrity:

Every update or transaction within the knowledge graph is digitally signed using robust public key infrastructure (PKI). This ensures that each action is authenticated and timestamped.

2. Blockchain Synchronization:
   A middleware layer periodically aggregates these digitally signed transactions and computes a cryptographic hash (e.g., via SHA-256). This hash is then committed to a block-chain sidechain (using an Ethereum-compatible protocol), providing a secure, decentralized record that guarantees data immutability without impacting real-time operations.
3. Dynamic Token-Based Licensing:
   The system includes a licensing module that evaluates usage metrics and transformation parameters to dynamically compute token costs for accessing the knowledge graphs. Smart contracts automatically manage token transfers, rewarding authors when users access their data.
4. Secure Authentication:
   The system employs a secure user authentication mechanism (e.g., OAuth 2.0 combined with multi-factor authentication) that links verified user identities to blockchain wallets, ensuring that all transactions and access rights are traceable.
5. Decentralized Governance:
   A decentralized decision-making process (resembling a DAO) allows domain experts to collectively manage, curate, and update their knowledge graphs. This maintains a human-centric approach to AI and prevents centralized control.

Further, domain experts engage with an AI-assisted training system that guides them in solving conceptual puzzles related to their field. As they input and modify data, the knowledge graph database captures each transaction. Simultaneously, the digital signature module signs every update, ensuring that each piece of information is authentic and traceable.

Further, the middleware layer continuously monitors the KG database for new transactions. At predetermined intervals, it aggregates these transactions and computes a secure cryptographic hash. This hash is then transmitted and committed to a block-chain

sidechain, creating an immutable audit trail without interrupting the performance of the live system.

Further, the token-based licensing module dynamically assesses how frequently and extensively the knowledge graph is accessed or transformed. Based on these metrics, it calculates token costs. When users access the KGs, smart contracts automatically deduct the requisite tokens from their linked block-chain wallets and credit the tokens to the domain experts' wallets.

Further, the authentication system ensures that every user accessing the system is verified through multi-factor authentication. This verified access links directly to block-chain wallets for seamless token transactions. Additionally, a decentralized governance module empowers domain experts to collaboratively manage and refine their taniners, ensuring that decisions about updates or licensing terms are made collectively.

Further, the system provides instructional content, interactive tutorials, and best-practice guidelines that help domain experts understand how to build and optimize their knowledge graphs. As experts gain experience, they can iteratively improve their taniners, using feedback from the decentralized governance process to refine their models further.

Further, the system may integrate quantum-resistant hashing algorithms, such as those based on lattice cryptography, to ensure that digital signatures remain secure against future cryptographic advancements. This feature addresses the technical problem of potential vulnerabilities in traditional hash functions by leveraging post-quantum cryptographic methods. In some embodiments, SHA-256 may be replaced with a lattice-based hash function like BLS (Boneh–Shoup).

Further, the system may incorporate biometric data to enhance key management scalability. This implementation allows users to establish cryptographic keys using fingerprints or facial recognition, reducing the reliance on traditional password-based systems and enhancing security. In some embodiments, multi-factor authentication (MFA) may be integrated with biometric verification for added layers of protection.

Further, the system may include a dynamic consent module to enable users to grant or revoke access dynamically. This feature addresses the technical problem of data privacy by allowing users to control which parts of their knowledge graph data are accessible. In

some embodiments, this module may use decentralized identifiers (DIDs) to enable self-sovereign identity management.

Further, the system may employ AI-driven anomaly detection to identify suspicious activities in real-time. This feature improves system reliability by detecting potential breaches or unauthorized access before they occur. In some embodiments, machine learning models may be trained on historical transaction data to predict and flag unusual patterns.

Further, the cross-chain compatibility may be integrated to allow the block-chain-audited digital signature system to operate across different block-chains. This feature addresses the technical problem of interoperability by enabling seamless integration with various block-chain networks, such as Bitcoin, Ethereum, and Tezos. In some embodiments, a Layer 2 solution may be used to bridge different chains while maintaining security.

Further, the system may leverage distributed ledger technology to enhance resilience against attacks. This feature improves fault tolerance by ensuring that no single point of failure can disrupt the network. In some embodiments, the knowledge graph database may be replicated across multiple nodes with automatic failover mechanisms.

Further, the system may include a peer-to-peer governance module to enable community-driven decision-making. This feature improves collaboration by allowing domain experts and users to vote on updates or ethical standards collectively. In some embodiments, this module may use a distributed ledger to record votes and ensure accountability.

Further, the system may employ privacy-preserving data aggregation techniques to protect sensitive information during knowledge graph updates. This feature improves data privacy by ensuring that aggregated data does not reveal individual user identities. In some embodiments, homomorphic encryption may be used to perform calculations on encrypted data without decrypting it.

Further, an adaptive performance optimization may be implemented to dynamically adjust system resources based on usage patterns. This feature improves scalability by allocating computing power and bandwidth only when needed. In some embodiments, AI-driven algorithms may predict peak usage times and preemptively scale resources.

Further, the system facilitates multi-stakeholder collaboration support to facilitate teamwork across domains. This feature improves decision-making by enabling multiple parties to contribute and validate updates or governance decisions. In some embodiments, a collaborative workspace may be created where stakeholders can review and approve changes using digital signatures.

FIG. 1 is an illustration of an online platform 100 consistent with various embodiments of the present disclosure. By way of non-limiting example, the online platform 100 may be hosted on a centralized server 102, such as, for example, a cloud computing service. The centralized server 102 may communicate with other network entities, such as, for example, a mobile device 106 (such as a smartphone, a laptop, a tablet computer etc.), other electronic devices 110 (such as desktop computers, server computers etc.), databases 114, and sensors 116 over a communication network 104, such as, but not limited to, the Internet. Further, users of the online platform 100 may include relevant parties such as, but not limited to, end-users, administrators, service providers, service consumers and so on. Accordingly, in some instances, electronic devices operated by the one or more relevant parties may be in communication with the platform.

A user 112, such as the one or more relevant parties, may access online platform 100 through a web based software application or browser. The web based software application may be embodied as, for example, but not be limited to, a website, a web application, a desktop application, and a mobile application compatible with a computing device 200.

With reference to FIG. 2, a system consistent with an embodiment of the disclosure may include a computing device or cloud service, such as computing device 200. In a basic configuration, computing device 200 may include at least one processing unit 202 and a system memory 204. Depending on the configuration and type of computing device, system memory 204 may comprise, but is not limited to, volatile (e.g. random-access memory (RAM)), non-volatile (e.g. read-only memory (ROM)), flash memory, or any combination. System memory 204 may include operating system 205, one or more programming modules 206, and may include a program data 207. Operating system 205, for example, may be suitable for controlling computing device 200’s operation. In one

embodiment, programming modules 206 may include image-processing module, machine learning module. Furthermore, embodiments of the disclosure may be practiced in conjunction with a graphics library, other operating systems, or any other application program and is not limited to any particular application or system. This basic configuration is illustrated in FIG. 2 by those components within a dashed line 208.

Computing device 200 may have additional features or functionality. For example, computing device 200 may also include additional data storage devices (removable and/or non-removable) such as, for example, magnetic disks, optical disks, or tape. Such additional storage is illustrated in FIG. 2 by a removable storage 209 and a non-removable storage 210. Computer storage media may include volatile and non-volatile, removable and non-removable media implemented in any method or technology for storage of information, such as computer-readable instructions, data structures, program modules, or other data. System memory 204, removable storage 209, and non-removable storage 210 are all computer storage media examples (i.e., memory storage.) Computer storage media may include, but is not limited to, RAM, ROM, electrically erasable read-only memory (EEPROM), flash memory or other memory technology, CD-ROM, digital versatile disks (DVD) or other optical storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other medium which can be used to store information and which can be accessed by computing device 200. Any such computer storage media may be part of device 200. Computing device 200 may also have input device(s) 212 such as a keyboard, a mouse, a pen, a sound input device, a touch input device, a location sensor, a camera, a biometric sensor, etc. Output device(s) 214 such as a display, speakers, a printer, etc. may also be included. The aforementioned devices are examples and others may be used.

Computing device 200 may also contain a communication connection 216 that may allow device 200 to communicate with other computing devices 218, such as over a network in a distributed computing environment, for example, an intranet or the Internet. Communication connection 216 is one example of communication media. Communication media may typically be embodied by computer readable instructions, data structures, program modules, or other data in a modulated data signal, such as a

carrier wave or other transport mechanism, and includes any information delivery media. The term "modulated data signal" may describe a signal that has one or more characteristics set or changed in such a manner as to encode information in the signal. By way of example, and not limitation, communication media may include wired media such as a wired network or direct-wired connection, and wireless media such as acoustic, radio frequency (RF), infrared, and other wireless media. The term computer readable media as used herein may include both storage media and communication media.

As stated above, a number of program modules and data files may be stored in system memory 204, including operating system 205. While executing on processing unit 202, programming modules 206 (e.g., application 220 such as a media player) may perform processes including, for example, one or more stages of methods, algorithms, systems, applications, servers, databases as described above. The aforementioned process is an example, and processing unit 202 may perform other processes. Other programming modules that may be used in accordance with embodiments of the present disclosure may include machine learning applications.

Generally, consistent with embodiments of the disclosure, program modules may include routines, programs, components, data structures, and other types of structures that may perform particular tasks or that may implement particular abstract data types. Moreover, embodiments of the disclosure may be practiced with other computer system configurations, including hand-held devices, general purpose graphics processor-based systems, multiprocessor systems, microprocessor-based or programmable consumer electronics, application specific integrated circuit-based electronics, minicomputers, mainframe computers, and the like. Embodiments of the disclosure may also be practiced in distributed computing environments where tasks are performed by remote processing devices that are linked through a communications network. In a distributed computing environment, program modules may be located in both local and remote memory storage devices.

Furthermore, embodiments of the disclosure may be practiced in an electrical circuit comprising discrete electronic elements, packaged or integrated electronic chips containing logic gates, a circuit utilizing a microprocessor, or on a single chip containing

electronic elements or microprocessors. Embodiments of the disclosure may also be practiced using other technologies capable of performing logical operations such as, for example, AND, OR, and NOT, including but not limited to mechanical, optical, fluidic, and quantum technologies. In addition, embodiments of the disclosure may be practiced within a general-purpose computer or in any other circuits or systems.

Embodiments of the disclosure, for example, may be implemented as a computer process (method), a computing system, or as an article of manufacture, such as a computer program product or computer readable media. The computer program product may be a computer storage media readable by a computer system and encoding a computer program of instructions for executing a computer process. The computer program product may also be a propagated signal on a carrier readable by a computing system and encoding a computer program of instructions for executing a computer process. Accordingly, the present disclosure may be embodied in hardware and/or in software (including firmware, resident software, micro-code, etc.). In other words, embodiments of the present disclosure may take the form of a computer program product on a computer-usable or computer-readable storage medium having computer-usable or computer-readable program code embodied in the medium for use by or in connection with an instruction execution system. A computer-usable or computer-readable medium may be any medium that can contain, store, communicate, propagate, or transport the program for use by or in connection with the instruction execution system, apparatus, or device.

The computer-usable or computer-readable medium may be, for example but not limited to, an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system, apparatus, device, or propagation medium. More specific computer-readable medium examples (a non-exhaustive list), the computer-readable medium may include the following: an electrical connection having one or more wires, a portable computer diskette, a random-access memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory (EPROM or Flash memory), an optical fiber, and a portable compact disc read-only memory (CD-ROM). Note that the computer-usable or computer-readable medium could even be paper or another suitable medium upon which

the program is printed, as the program can be electronically captured, via, for instance, optical scanning of the paper or other medium, then compiled, interpreted, or otherwise processed in a suitable manner, if necessary, and then stored in a computer memory.

Embodiments of the present disclosure, for example, are described above with reference to block diagrams and/or operational illustrations of methods, systems, and computer program products according to embodiments of the disclosure. The functions/acts noted in the blocks may occur out of the order as shown in any flowchart. For example, two blocks shown in succession may in fact be executed substantially concurrently or the blocks may sometimes be executed in the reverse order, depending upon the functionality/acts involved.

While certain embodiments of the disclosure have been described, other embodiments may exist. Furthermore, although embodiments of the present disclosure have been described as being associated with data stored in memory and other storage mediums, data can also be stored on or read from other types of computer-readable media, such as secondary storage devices, like hard disks, solid state storage (e.g., USB drive), or a CD-ROM, a carrier wave from the Internet, or other forms of RAM or ROM. Further, the disclosed methods' stages may be modified in any manner, including by reordering stages and/or inserting or deleting stages, without departing from the disclosure.

Fig. 3 illustrates a flowchart of a method 300 for facilitating decentralized management of a knowledge graph, in accordance with some embodiments.

Accordingly, the method 300 may include a step 302 of receiving, using a communication device 1202, a domain data from a user device associated with a user. Further, the domain data corresponds to a subject matter within a domain. Further, the method 300 may include a step 304 of analyzing, using a processing device 1204, the domain data. Further, the method 300 may include a step 306 of generating, using the processing device 1204, a knowledge graph operation data based on the analyzing. Further, the knowledge graph operation data includes one or more of a creation data which may be configured for creating a knowledge graph data and an updation data which may be configured for updating the knowledge graph data. Further, the method

300 may include a step 308 of executing, using the processing device 1204, one or more of the creating and the updating. Further, the method 300 may include a step 310 of storing, using a storage device 1206, the knowledge graph operation data on a decentralized database.

Fig. 4 illustrates a flowchart of a method 400 for facilitating decentralized management of a knowledge graph including generating, using the processing device 1204, a response data, in accordance with some embodiments.

Further, in some embodiments, the method 400 further may include a step 402 of instantiating, using the processing device 1204, a transformation agent which may be configured to access the knowledge graph data. Further, in some embodiments, the method 400 further may include a step 404 of receiving, using the communication device 1202, a query data from a second user device associated with a second user. Further, the query data includes a query associated with the knowledge graph data. Further, in some embodiments, the method 400 further may include a step 406 of processing, using the processing device 1204, the query data based on the transformation agent. Further, in some embodiments, the method 400 further may include a step 408 of generating, using the processing device 1204, a response data based on the processing. Further, the response data includes a response to the query. Further, in some embodiments, the method 400 further may include a step 410 of transmitting, using the communication device 1202, the response data to the second user device.

Fig. 5 illustrates a flowchart of a method 500 for facilitating decentralized management of a knowledge graph including retraining, using the processing device 1204, the transformation agent, in accordance with some embodiments.

Further, in some embodiments, the method 500 further may include a step 502 of receiving, using the communication device 1202, a feedback data from the second user device. Further, the feedback data includes a feedback corresponding to the response data. Further, in some embodiments, the method 500 further may include a step 504 of storing, using the storage device 1206, each of the response data and the feedback data on the decentralized database. Further, in some embodiments, the method 500 further may

include a step 506 of retraining, using the processing device 1204, the transformation agent based on the feedback data.

Fig. 6 illustrates a flowchart of a method 600 for facilitating decentralized management of a knowledge graph including retraining, using the processing device 1204, the transformation agent, in accordance with some embodiments.

Further, in some embodiments, the method 600 further may include a step 602 of determining, using the processing device 1204, a performance data based on the response data. Further, the performance data corresponds to a performance of the transformative agent. Further, in some embodiments, the method 600 further may include a step 604 of storing, using the storage device 1206, each of the response data and the performance data on the decentralized database. Further, in some embodiments, the method 600 further may include a step 606 of retraining, using the processing device 1204, the transformation agent based on the performance data.

Fig. 7 illustrates a flowchart of a method 700 for facilitating decentralized management of a knowledge graph including retraining, using the processing device 1204, the transformation agent, in accordance with some embodiments.

Further, in some embodiments, the method 700 further may include a step 702 of determining, using the processing device 1204, an ethical data based on the query data. Further, the ethical data corresponds to an ethical standard associated with a domain of the query. Further, in some embodiments, the method 700 further may include a step 704 of analyzing, using the processing device 1204, the response data based on the ethical data. Further, in some embodiments, the method 700 further may include a step 706 of generating, using the processing device 1204, an ethical feedback data based on the analyzing of the response data. Further, the ethical feedback data includes a feedback corresponding to an ethical compliance of the response. Further, in some embodiments, the method 700 further may include a step 708 of retraining, using the processing device 1204, the transformation agent based on the ethical feedback data.

Fig. 8 illustrates a flowchart of a method 800 for facilitating decentralized management of a knowledge graph including analyzing, using the processing device 1204, the validation data, in accordance with some embodiments.

Further, in some embodiments, the method 800 further may include a step 802 of receiving, using the communication device 1202, a validation data from a second expert device associated with a second domain expert. Further, the validation data corresponds to a validation of the ethical standard. Further, in some embodiments, the method 800 further may include a step 804 of analyzing, using the processing device 1204, the validation data. Further, the determining of the ethical data may be further based on the validation data. Further, in some embodiments, the method 800 further may include a step 806 of storing, using the storage device 1206, the validation data in the decentralized database.

Fig. 9 illustrates a flowchart of a method 900 for facilitating decentralized management of a knowledge graph including generating, using the processing device 1204, an agent data, in accordance with some embodiments.

Further, in some embodiments, the method 900 further may include a step 902 of generating, using the processing device 1204, an agent data. Further, the agent data includes an executable code. Further, the executable code corresponds to the transformation agent. Further, in some embodiments, the method 900 further may include a step 904 of storing, using the storage device 1206, the agent data in the decentralized database.

Fig. 10 illustrates a flowchart of a method 1000 for facilitating decentralized management of a knowledge graph including generating, using the processing device 1204, a reward data, in accordance with some embodiments.

Further, in some embodiments, the method 1000 further may include a step 1002 of generating, using the processing device 1204, a reward data based on the knowledge graph operation data. Further, the reward data includes a reward token for a transaction of the knowledge graph data. Further, in some embodiments, the method 1000 further may

include a step 1004 of transmitting, using the communication device 1202, the reward data to the user device.

Fig. 11 illustrates a flowchart of a method 1100 for facilitating decentralized management of a knowledge graph including generating, using the processing device 1204, a signature data, in accordance with some embodiments.

Further, in some embodiments, the method 1100 further may include a step 1102 of receiving, using the communication device 1202, an authentication data from the user device. Further, the authentication data includes a unique identifier of the user. Further, in some embodiments, the method 1100 further may include a step 1104 of analyzing, using the processing device 1204, the authentication data. Further, in some embodiments, the method 1100 further may include a step 1106 of generating, using the processing device 1204, a hash data based on the knowledge graph operation data. Further, the hash data includes a hash value comprising each of two or more alphabets and two or more numericals. Further, the hash value represents a transaction of the knowledge graph data. Further, in some embodiments, the method 1100 further may include a step 1108 of generating, using the processing device 1204, a signature data based on each of the hash data and the analyzing of the authentication data. Further, the signature may data includes a digital signature representing the user associated with the transaction. Further, in some embodiments, the method 1100 further may include a step 1110 of storing, using the storage device 1206, the signature data on the decentralized database.

In some embodiments, the knowledge graph data includes a domain specific knowledge graph in a human-readable format. Further, the human-readable format includes one or more of a natural language format, a structured text format and a visual format.

Fig. 12 illustrates a block diagram of a system 1200 for facilitating decentralized management of a knowledge graph, in accordance with some embodiments.

Accordingly, the system 1200 may include a communication device 1202. Further, the communication device 1202 may be configured for receiving a domain data from a user device associated with a user. Further, the domain data corresponds to a subject

matter within a domain. Further, the system 1200 may include a processing device 1204 communicatively coupled with the communication device 1202. Further, the processing device 1204 may be configured for analyzing the domain data. Further, the processing device 1204 may be configured for generating a knowledge graph operation data based on the analyzing. Further, the knowledge graph operation data includes one or more of a creation data which may be configured for creating a knowledge graph data and an updation data which may be configured for updating the knowledge graph data. Further, the processing device 1204 may be configured for executing one or more of the creating and the updating. Further, the system 1200 may include a storage device 1206 which may be configured for storing the knowledge graph operation data on a decentralized database.

Further, in some embodiments, the communication device 1202 may be further configured for receiving a query data from a second user device associated with a second user. Further, the query data includes a query associated with the knowledge graph data. Further, the communication device 1202 may be further configured for transmitting a response data to the second user device. Further, the processing device 1204 may be further configured for instantiating a transformation agent which may be configured to access the knowledge graph data. Further, the processing device 1204 may be further configured for processing the query data based on the transformation agent. Further, the processing device 1204 may be further configured for generating the response data based on the processing. Further, the response data includes a response to the query.

In some embodiments, the communication device 1202 may be further configured for receiving a feedback data from the second user device. Further, the feedback data includes a feedback corresponding to the response data. Further, the storage device 1206 may be further configured for storing each of the response data and the feedback data on the decentralized database. Further, the processing device 1204 may be further configured for retraining the transformation agent based on the feedback data.

Further, in some embodiments, the processing device 1204 may be further configured for determining a performance data based on the response data. Further, the performance data corresponds to a performance of the transformative agent. Further, the processing

device 1204 may be further configured for retraining the transformation agent based on the performance data. Further, the storage device 1206 may be further configured for storing each of the response data and the performance data on the decentralized database.

Further, in some embodiments, the processing device 1204 may be further configured for determining an ethical data based on the query data. Further, the ethical data corresponds to an ethical standard associated with a domain of the query. Further, the processing device 1204 may be further configured for analyzing the response data based on the ethical data. Further, the processing device 1204 may be further configured for generating an ethical feedback data based on the analyzing of the response data. Further, the ethical feedback data includes a feedback corresponding to an ethical compliance of the response. Further, the processing device 1204 may be further configured for retraining the transformation agent based on the ethical feedback data.

In some embodiments, the communication device 1202 may be further configured for receiving a validation data from a second expert device associated with a second domain expert. Further, the validation data corresponds to a validation of the ethical standard. Further, the processing device 1204 may be further configured for analyzing the validation data. Further, the determining of the ethical data may be further based on the validation data. Further, the storage device 1206 may be further configured for storing the validation data in the decentralized database.

In some embodiments, the processing device 1204 may be further configured for generating an agent data. Further, the agent data includes an executable code. Further, the executable code corresponds to the transformation agent. Further, the storage device 1206 may be further configured for storing the agent data in the decentralized database.

In some embodiments, the processing device 1204 may be further configured for generating a reward data based on the knowledge graph operation data. Further, the reward data includes a reward token for a transaction of the knowledge graph data. Further, the communication device 1202 may be further configured for transmitting the reward data to the user device.

Further, in some embodiments, the communication device 1202 may be further configured for receiving an authentication data from the user device. Further, the authentication data may include a unique identifier of the user. Further, the processing device 1204 may be further configured for analyzing the authentication data. Further, the communication device 1202 may be further configured for receiving an authentication data from the user device. Further, the processing device 1204 may be further configured for generating a hash data based on the knowledge graph operation data. Further, the hash data includes a hash value comprising each of two or more alphabets and two or more numericals. Further, the hash value represents a transaction of the knowledge graph data. Further, the communication device 1202 may be further configured for receiving an authentication data from the user device. Further, the processing device 1204 may be further configured for generating a signature data based on each of the hash data and the analyzing of the authentication data. Further, the signature may data includes a digital signature representing the user associated with the transaction. Further, the storage device 1206 may be further configured for storing the signature data on the decentralized database.

In some embodiments, the knowledge graph data includes a domain specific knowledge graph in a human-readable format. Further, the human-readable format includes one or more of a natural language format, a structured text format and a visual format.

In some embodiments, the knowledge graph data includes a domain-specific knowledge graph representing a relationship between two or more components of the subject matter.

In some embodiments, the generating of the knowledge graph operation data may be further based on AI model.

In some embodiments, the decentralized database may be configured to be accessible to two or more users based on two or more authentication data.

In some embodiments, the generating of the signature data includes encrypting the hash value based on the unique identifier to obtain an encrypted hash value. Further, the digital signature includes the encrypted hash value.

In some embodiments, the unique identifier includes a private key assigned to the user.

In some embodiments, the transaction represents one or more of the creating and the updating.

Fig. 13 illustrates a flowchart of a method 1300 for facilitating decentralized management of a knowledge graph including generating, using the processing device 1204, a time data, in accordance with some embodiments.

Further, in some embodiments, the method 1300 further may include a step 1302 of generating, using the processing device 1204, a time data based on the knowledge graph operation data. Further, the time data represents a time instance at which a transaction of the knowledge graph data occurred. Further, in some embodiments, the method 1300 further may include a step 1304 of storing, using the processing device 1204, the time data in the decentralized database.

In some embodiments, the knowledge graph data may be represented with one or more of the time value and the digital signature.

In some embodiments, the visual format corresponds to a diagram comprising one or more of two or more nodes and two or more edges.

In some embodiments, the two or more nodes represents two or more components. Further, the two or more edges represents a relationship between the two or more components.

In some embodiments, the structured text corresponds to a table representing the two or more components.

In some embodiments, the executable code includes a script based on a programming language.

In some embodiments, the programming language includes one or more of a groovy language and a python language.

Fig. 14 illustrates a flowchart of a method 1400 for facilitating decentralized management of a knowledge graph including generating, using the processing device 1204, a configuration data, in accordance with some embodiments.

Further, in some embodiments, the method 1400 further may include a step 1402 of generating, using the processing device 1204, a configuration data based on the agent data. Further, the configuration data represents one or more of a parameter of the executable code and a configuration of the executable code. Further, in some embodiments, the method 1400 further may include a step 1404 of storing, using the storage device 1206, the configuration data in the decentralized database.

In some embodiments, the parameter corresponds to at least of an acceptable input of the executable code and an operation performable by the executable code.

In some embodiments, the decentralized database includes one or more of a first decentralized database and a second decentralized database.

In some embodiments, the first decentralized database and the second decentralized database corresponds to a main block-chain and a side block-chain respectively.

In some embodiments, each of the main block-chain and the side block-chain includes a network of plurality of blocks.

In some embodiments, the two or more authentication data based accessings of the knowledge graph data ensures one or more of an integrity of a domain specific knowledge graph and an accountability of the domain specific knowledge graph.

In some embodiments, the user includes a domain expert.

In some embodiments, the decentralized database includes two or more hash values representing two or more transactions.

In some embodiments, the reward token represents an ownership of the transaction.

In some embodiments, the reward token includes a cryptocurrency.

In some embodiments, the instantiating of the transformative agent includes one or more of a retrieving the transformative agent and compiling the transformative agent.

In some embodiments, the transformative agent may be configured to perform a task based on the knowledge graph data.

In some embodiments, the task includes solving a complex problem based on the knowledge graph data. Further, the complex problem may be associated with the domain.

Fig. 15 illustrates a flowchart of a method 1500 for facilitating decentralized management of a knowledge graph including generating, using the processing device 1204, a cost data, in accordance with some embodiments.

Further, in some embodiments, the method 1500 further may include a step 1502 of generating, using the processing device 1204, a cost data based on the processing of the query data. Further, the cost data represents a payable amount for an access token to access one or more of the response and the knowledge graph data. Further, in some embodiments, the method 1500 further may include a step 1504 of transmitting, using the communication device 1202, the cost data to the second user device.

Fig. 16 illustrates a flowchart of a method 1600 for facilitating decentralized management of a knowledge graph including generating, using the processing device 1204, an access token data, in accordance with some embodiments.

Further, in some embodiments, the method 1600 further may include a step 1602 of receiving, using the processing device 1204, an initiation data from the second user device. Further, the initiation data represents one or more of a payment method and a payment detail. Further, in some embodiments, the method 1600 further may include a step 1604 of processing, using the processing device 1204, a transaction based on the initiation data. Further, in some embodiments, the method 1600 further may include a step 1606 of generating, using the processing device 1204, an access token data based on the processing. Further, the access token data includes the access token for accessing one or more of the response and the knowledge graph data. Further, in some embodiments,

the method 1600 further may include a step 1608 of transmitting, using the communication device 1202, an access token data to the second user device.

In some embodiments, the access token data includes two or more access tokens for accessing one or more of the response and the knowledge graph data at two or more time instances over a time interval.

In some embodiments, the processing of the query data includes determining one or more of a complexity of the response and an operation associated with the response. Further, the payable amount may be further based on one or more of the complexity and the operation.

In some embodiments, the method 1500 may further include generating, using the processing device 1204, a usage metric data based on the response data. Further, the usage metric data includes a metric corresponding a parameter associated with the response data. Further, the generating of the cost data may be further based on the usage metric data.

In some embodiments, the parameter includes a time duration of a second user engagement with the transformation agent.

In some embodiments, the metric includes a real-time usage metric.

In some embodiments, the generating of the reward data may be further based on an executing of an executable agreement code which may be configured to execute based on a predetermined agreement.

In some embodiments, the predetermined agreement represents a requirement for the reward token.

In some embodiments, the executable agreement code may be stored in the decentralized database.

In some embodiments, the generating of the access token data may be further based on an executing of the executable agreement code, the predetermined agreement represents the requirement for the access token.

In some embodiments, the executable agreement code may be configured to deduct a count of the access token based on the second user engagement with one or more of the response data and the knowledge graph data.

Fig. 17 illustrates a flowchart of a method 1700 for facilitating decentralized management of a knowledge graph including analyzing, using the processing device 1204, the access token data, in accordance with some embodiments.

Further, in some embodiments, the method 1700 further may include a step 1702 of receiving, using the communication device 1202, an access token data from the second user device. Further, the access token data includes an access token for accessing one or more of the response data and the knowledge graph data. Further, in some embodiments, the method 1700 further may include a step 1704 of analyzing, using the processing device 1204, the access token data. Further, the processing of the query data may be further based on the analyzing of the access token data.

In some embodiments, the validation data includes two or more validation data received from two or more expert devices.

In some embodiments, the two or more validation data includes two or more validations comprising two or more votes.

In some embodiments, the determining of the ethical data may be based on a voting mechanism.

In some embodiments, the determining based on the analyzing of the two or more validation data facilitates a decentralized governance.

In some embodiments, the transformation agent may be configured to adapt based on the ethical feedback data.

In some embodiments, the ethical standard corresponds to one or more of a moral dilemma, a logical fallacy and a sample argument.

In some embodiments, the analyzing of the response data may be further based on one or more of an Aristotelian logic, a Socratic dialectic inquiry, and a Wittgensteinian language game.

Fig. 18 illustrates a flowchart of a method 1800 for facilitating decentralized management of a knowledge graph including retrieving, using the processing device 1204, the transformation agent from a plurality of transformation agents, in accordance with some embodiments.

Further, in some embodiments, the method 1800 further may include a step 1802 of analyzing, using the processing device 1204, the query data. Further, in some embodiments, the method 1800 further may include a step 1804 of retrieving, using the processing device 1204, the transformation agent from two or more transformation agents based on the analyzing of the query data. Further, the processing of the response data may be based on the retrieving.

In some embodiments, the performance data corresponds to the retrieving of the transformative agent.

In some embodiments, the processing of the query data may be based on two or more transformative agents. Further, the performance data corresponds to a refinement of a combination of the two or more transformative agents.

In some embodiments, the transformative agent may be configured for an adaptive learning based on the feedback data. Further, the adaptive learning facilitates a dynamic response generation.

Fig. 19 illustrates a flowchart of a method 1900 for facilitating decentralized management of a knowledge graph including training, using the processing device 1204, the transformation agent, in accordance with some embodiments.

Further, in some embodiments, the method 1900 further may include a step 1902 of generating, using the processing device 1204, a foundational data. Further, the foundation data includes a foundational knowledge graph. Further, in some embodiments, the method 1900 further may include a step 1904 of training, using the processing device

1204, the transformation agent based on the foundational data. Further, the transformation agent may be configured to learn based on the foundational knowledge graph.

In some embodiments, the foundational knowledge graph includes one or more of an abstraction and reasoning corpus puzzle knowledge graph and a mathematics knowledge graph.

In some embodiments, the foundation data further includes a puzzle derived from one or more of a training dataset and an evaluation dataset.

In some embodiments, the analyzing of the domain data may be based on a large language model.

In some embodiments, the method 400 may further include generating, using the processing device 1204, a command data based on the query data. Further, the command data includes a cypher command. Further, the processing of the query data includes processing of the command data.

In some embodiments, the method 700 may further include receiving, using the communication device 1202, a modified ethical data from the user device. Further, the modified ethical data includes a modified ethical standard. Further, the analyzing of the response data may be further based on the modified ethical data.

In some embodiments, the validation data corresponds to the validation of a parameter associated with the transformative agent.

In some embodiments, the method 400 may be further include retrieving, using the processing device 1204, a contextual data based on the processing. Further, the contextual data includes an external detail corresponding to the query. Further, the generating of the response data may be further based on the contextual data.

In some embodiments, the contextual data may be retrieved form an external database through an application programing interface.

In some embodiments, the external database corresponds to an enterprise.

In some embodiments, the method 700 may further include transmitting, using the communication device 1202, the ethical feedback data to the user device. Further, the ethical feedback data represents a non-compliance of the response data for an expert review.

In some embodiments, the method 1600 may be the executable agreement code may be configured to automate a micro transaction.

In some embodiments, the method 600 may further include generating, using the processing device 1204, a modified agent data based on one or more of the performance data and the feedback data. Further, the modified agent data includes a modified executable code of the transformation agent. Further, the generating of the response data at a second time instance may be based on the modified executable code. Further, each of the performance data and the feedback data may be based on the response data generated at the first time instance.

In some embodiments, the second time instance occurred later than the first time instance.

In some embodiments, the query data corresponds to one or more of an abstract puzzle, a complex mathematical problem, and an ethical language game.

In some embodiments, the generating of the hash data may be based on a cryptographic hash function.

In some embodiments, the cryptographic hash function includes a secure hash algorithm.

In some embodiments, the method 1700 may further include storing, using the processing device 1204, the access token data in the decentralized database.

Fig. 20 illustrates a system architecture, in accordance with some embodiments. Further, the system includes a knowledge graph database 2002 to store domain-specific data as a knowledge graph comprising an interconnected node and edge. Further, knowledge graph transaction is digitally signed and timestamped. Further, the system

includes a digital signature module 2004 for generating digital signature for knowledge graph transaction based on a public key infrastructure. Further, the system includes a block-chain synchronization module 2006 for one or more of aggregating knowledge graph transaction and computing a cryptographic hash. Further, the system includes a token-based licensing module 2008 for calculating token cost based on real-time usage metric. Further, the system includes a decentralized governance module 2010 for providing a voting mechanism through which domain experts can validate the knowledge graph. Further, the system includes a secure authentication module 2012 for implementing multi-factor authentication.

Fig. 21 illustrates a flowchart of decentralized management of a knowledge graph, in accordance with some embodiments. Further, the decentralized management include one or more of a step 2102 of constructing a knowledge graph, a step 2104 of recording a transaction in knowledge graph, a step 2106 of enforcing a top node security, a step 2108 of one or more of aggregating the transaction and computing a hash, a step 2110 of synchronizing the hash to block-chain, a step 2112 of dynamic token-based licensing, a step 2114 of decentralized governance, and a step 2116 of securing and monetizing an access of the knowledge graph.

Fig. 22 illustrates a top node schematic of decentralized management of a knowledge graph, in accordance with some embodiments. Further, an enhanced top node module 2202 may utilize one of more of a token gating mechanism 2204, a usage metric 2206, and a digital signature 2208. Further, the enhanced top node module 2202 facilitates a secure access to a knowledge graph 2210.

Although the invention has been explained in relation to its preferred embodiment, it is to be understood that many other possible modifications and variations can be made without departing from the spirit and scope of the invention as hereinafter claimed.

CLAIMS

1. A method for facilitating decentralized management of a knowledge graph, the method comprising:

receiving, using a communication device, a domain data from a user device associated with a user, wherein the domain data corresponds to a subject matter within a domain;

analyzing, using a processing device, the domain data;

generating, using the processing device, a knowledge graph operation data based on the analyzing, wherein the knowledge graph operation data comprises at least one of a creation data configured for creating a knowledge graph data and an updation data configured for updating the knowledge graph data;

executing, using the processing device, at least one of the creating and the updating; and

storing, using a storage device, the knowledge graph operation data on a decentralized database.

2. The method of claim 1 further comprising:

instantiating, using the processing device, a transformation agent configured to access the knowledge graph data;

receiving, using the communication device, a query data from a second user device associated with a second user, wherein the query data comprises a query associated with the knowledge graph data;

processing, using the processing device, the query data based on the transformation agent;

generating, using the processing device, a response data based on the processing, wherein the response data comprises a response to the query; and

transmitting, using the communication device, the response data to the second user device.

3. The method of claim 2 further comprising:

receiving, using the communication device, a feedback data from the second user device, wherein the feedback data comprises a feedback corresponding to the response data;

storing, using the storage device, each of the response data and the feedback data on the decentralized database; and

retraining, using the processing device, the transformation agent based on the feedback data.

4. The method of claim 2 further comprising:

determining, using the processing device, a performance data based on the response data, wherein the performance data corresponds to a performance of the transformative agent;

storing, using the storage device, each of the response data and the performance data on the decentralized database; and

retraining, using the processing device, the transformation agent based on the performance data.

5. The method of claim 2 further comprises:

determining, using the processing device, an ethical data based on the query data, wherein the ethical data corresponds to an ethical standard associated with a domain of the query;

analyzing, using the processing device, the response data based on the ethical data;

generating, using the processing device, an ethical feedback data based on the analyzing of the response data, wherein the ethical feedback data comprises a feedback corresponding to an ethical compliance of the response; and

retraining, using the processing device, the transformation agent based on the ethical feedback data.

6. The method of claim 5 further comprises:

receiving, using the communication device, a validation data from a second expert device associated with a second domain expert, wherein the validation data corresponds to a validation of the ethical standard; and

analyzing, using the processing device, the validation data, wherein the determining of the ethical data is further based on the validation data; and

storing, using the storage device, the validation data in the decentralized database.

7. The method of claim 2 further comprises:

generating, using the processing device, an agent data, wherein the agent data comprises an executable code, wherein the executable code corresponds to the transformation agent; and

storing, using the storage device, the agent data in the decentralized database.

8. The method of claim 1 further comprises:

generating, using the processing device, a reward data based on the knowledge graph operation data, wherein the reward data comprises a reward token for a transaction of the knowledge graph data; and

transmitting, using the communication device, the reward data to the user device.

9. The method of claim 1 further comprises:

receiving, using the communication device, an authentication data from the user device, wherein the authentication data comprises a unique identifier of the user;

analyzing, using the processing device, the authentication data;

generating, using the processing device, a hash data based on the knowledge graph operation data, wherein the hash data comprises a hash value comprising each of a plurality of alphabets and a plurality of numericals, wherein the hash value represents a transaction of the knowledge graph data;

generating, using the processing device, a signature data based on each of the hash data and the analyzing of the authentication data, wherein the signature data comprises a digital signature representing the user associated with the transaction; and

storing, using the storage device, the signature data on the decentralized database.

10. The method of claim 1, wherein the knowledge graph data comprises a domain specific knowledge graph in a human-readable format, wherein the human-readable format comprises at least one of a natural language format, a structured text format and a visual format.

11. A system for facilitating decentralized management of a knowledge graph, the system comprising:

a communication device configured for:

receiving a domain data from a user device associated with a user, wherein the domain data corresponds to a subject matter within a domain;

a processing device configured for:

analyzing the domain data;

generating a knowledge graph operation data based on the analyzing, wherein the knowledge graph operation data comprises at least one of a creation data configured for creating a knowledge graph data and an updation data configured for updating the knowledge graph data;

executing at least one of the creating and the updating; and

a storage device configured for storing the knowledge graph operation data on a decentralized database.

12. The system of claim 11, wherein the communication device is further configured for:

receiving a query data from a second user device associated with a second user, wherein the query data comprises a query associated with the knowledge graph data;

transmitting a response data to the second user device, wherein the processing device is further configured for:

instantiating a transformation agent configured to access the knowledge graph data;

processing the query data based on the transformation agent; and

generating the response data based on the processing, wherein the response data comprises a response to the query.

13. The system of claim 12, wherein the communication device is further configured for receiving a feedback data from the second user device, wherein the feedback data comprises a feedback corresponding to the response data, wherein the storage device is further configured for storing each of the response data and the feedback data on the decentralized database, wherein the processing device is further configured for retraining the transformation agent based on the feedback data.

14. The system of claim 12, wherein the processing device is further configured for:

determining a performance data based on the response data, wherein the performance data corresponds to a performance of the transformative agent; and

retraining the transformation agent based on the performance data, wherein the storage device is further configured for storing each of the response data and the performance data on the decentralized database.

15. The system of claim 12, wherein the processing device is further configured for:

determining an ethical data based on the query data, wherein the ethical data corresponds to an ethical standard associated with a domain of the query;

analyzing the response data based on the ethical data;

generating an ethical feedback data based on the analyzing of the response data, wherein the ethical feedback data comprises a feedback corresponding to an ethical compliance of the response; and

retraining the transformation agent based on the ethical feedback data.

16. The system of claim 15, wherein the communication device is further configured for receiving a validation data from a second expert device associated with a second domain expert, wherein the validation data corresponds to a validation of the ethical standard, wherein the processing device is further configured for analyzing the validation data, wherein the determining of the ethical data is further based on the validation data, wherein the storage device is further configured for storing the validation data in the decentralized database.

17. The system of claim 12, wherein the processing device is further configured for generating an agent data, wherein the agent data comprises an executable code, wherein the executable code corresponds to the transformation agent, wherein the storage device is further configured for storing the agent data in the decentralized database.

18. The system of claim 11, wherein the processing device is further configured for generating a reward data based on the knowledge graph operation data, wherein the reward data comprises a reward token for a transaction of the knowledge graph data, wherein the communication device is further configured for transmitting the reward data to the user device.

19. The system of claim 11, wherein the communication device is further configured for receiving an authentication data from the user device, wherein the authentication data comprises a unique identifier of the user, wherein the processing device is further configured for:

analyzing the authentication data;

generating a hash data based on the knowledge graph operation data, wherein the hash data comprises a hash value comprising each of a plurality of alphabets and a plurality of numericals, wherein the hash value represents a transaction of the knowledge graph data; and

generating a signature data based on each of the hash data and the analyzing of the authentication data, wherein the signature data comprises a digital signature representing the user associated with the transaction, wherein the storage device is further configured for storing the signature data on the decentralized database.

20. The system of claim 11, wherein the knowledge graph data comprises a domain specific knowledge graph in a human-readable format, wherein the human-readable format comprises at least one of a natural language format, a structured text format and a visual format.

ABSTRACT

The present disclosure provides a method for facilitating decentralized management of a knowledge graph. Further, the method may include receiving a domain data from a user device associated with a user. Further, the domain data corresponds to a subject matter within a domain. Further, the method may include analyzing the domain data. Further, the method may include generating a knowledge graph operation data based on the analyzing. Further, the knowledge graph operation data includes one or more of a creation data which may be configured for creating a knowledge graph data and an updation data which may be configured for updating the knowledge graph data. Further, the method may include executing one or more of the creating and the updating. Further, the method may include storing the knowledge graph operation data on a decentralized database.

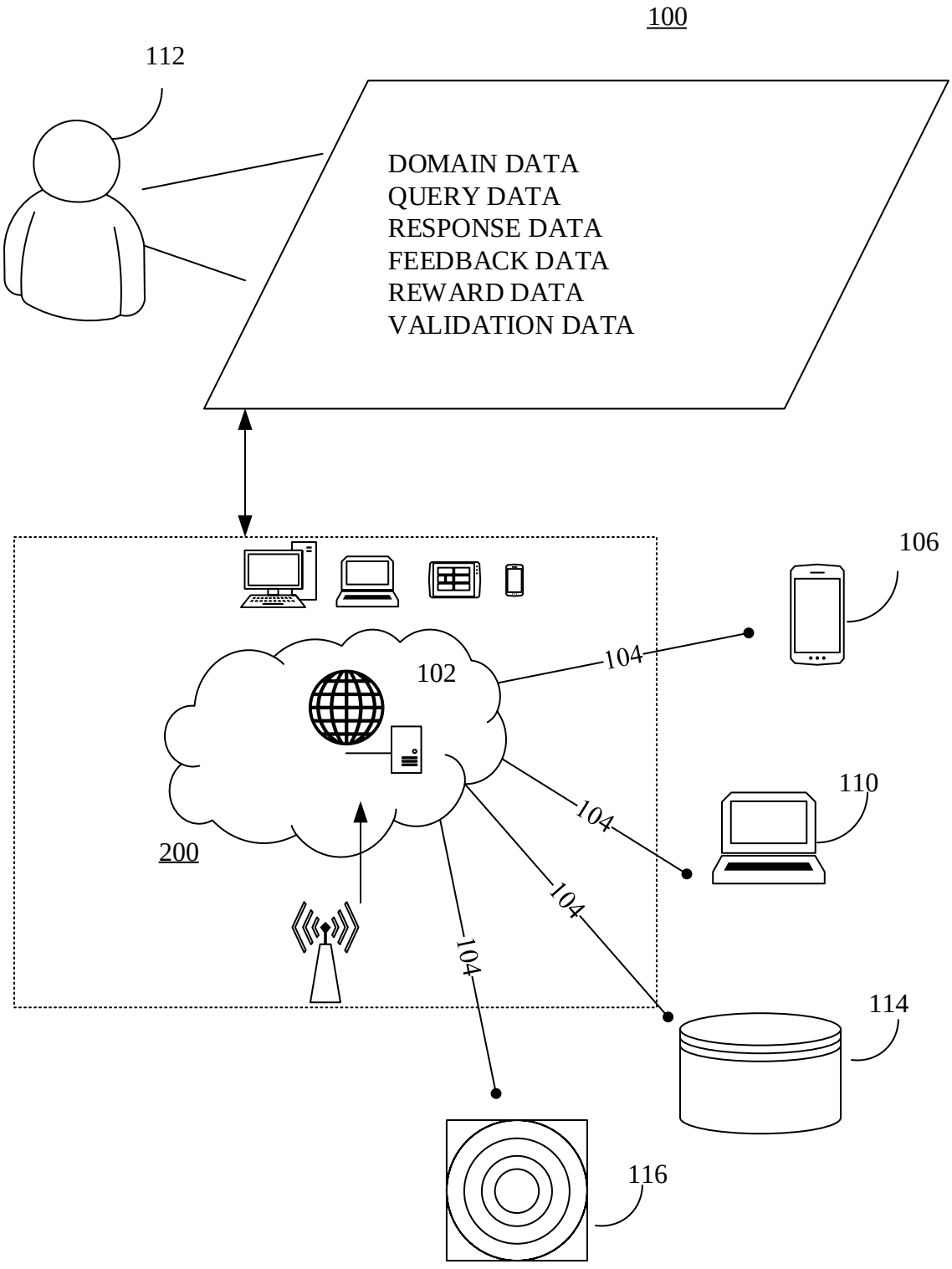

100
112
DOMAIN DATA
QUERY DATA
RESPONSE DATA
FEEDBACK DATA
REWARD DATA
VALIDATION DATA
106
102
104
110
200
104
104
104
114
116

Fig. 1

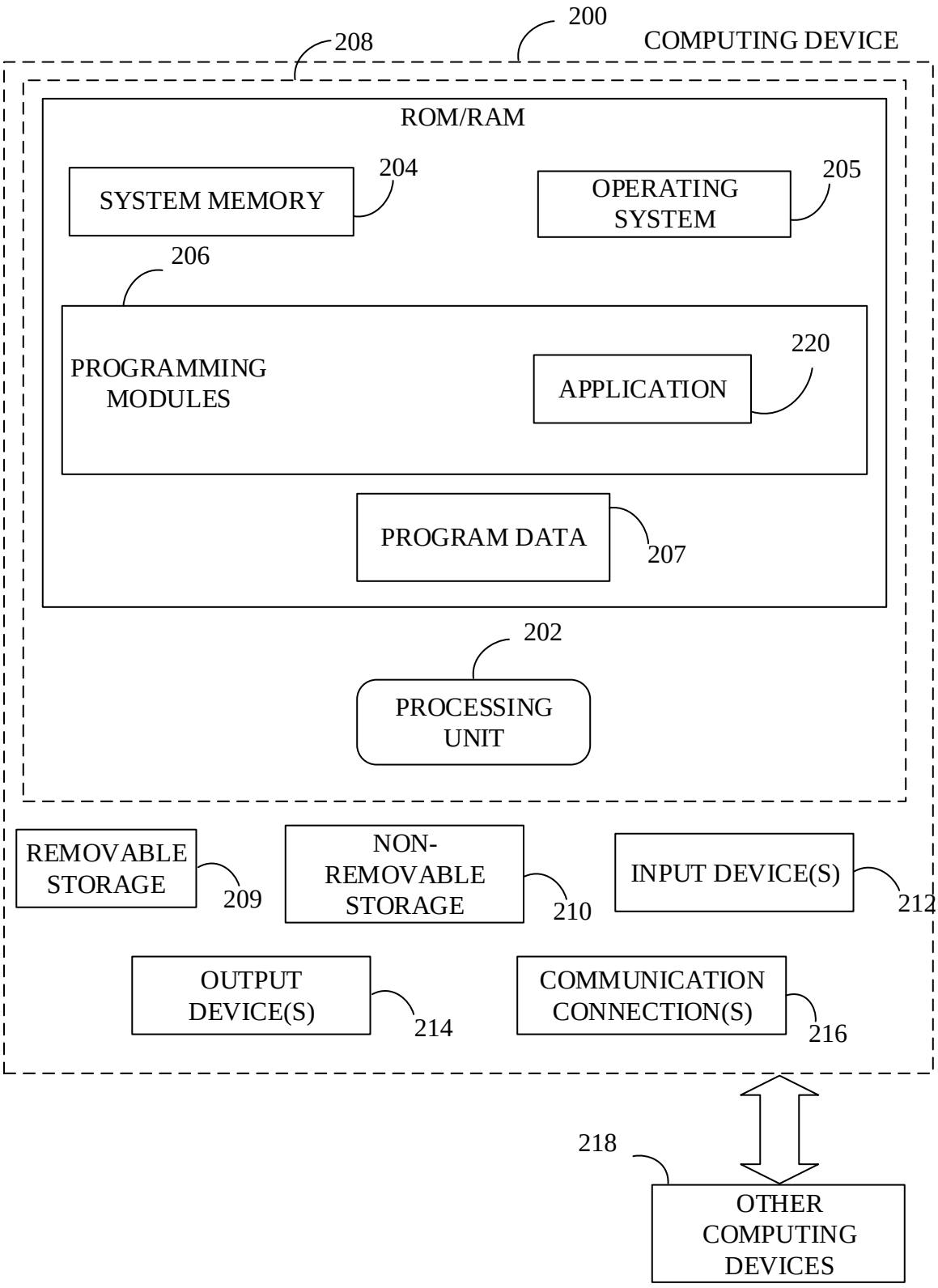

200
COMPUTING DEVICE
208
ROM/RAM
SYSTEM MEMORY
204
OPERATING SYSTEM
205
206
PROGRAMMING MODULES
220
APPLICATION
PROGRAM DATA
207
202
PROCESSING UNIT
REMOVABLE STORAGE
209
NON-REMOVABLE STORAGE
210
INPUT DEVICE(S)
212
OUTPUT DEVICE(S)
214
COMMUNICATION CONNECTION(S)
216
218
OTHER COMPUTING DEVICES

Fig. 2

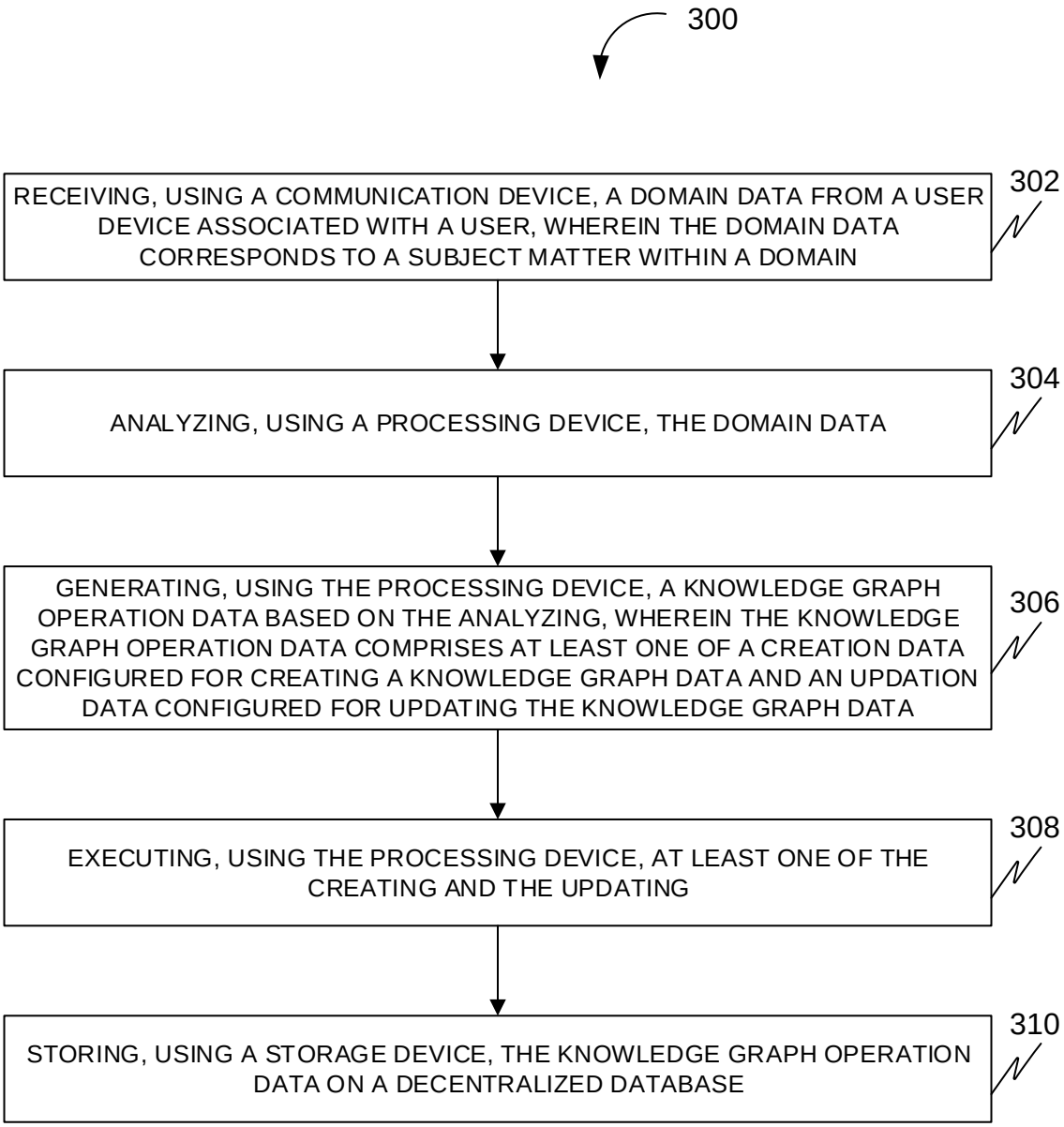

300
RECEIVING, USING A COMMUNICATION DEVICE, A DOMAIN DATA FROM A USER DEVICE ASSOCIATED WITH A USER, WHEREIN THE DOMAIN DATA CORRESPONDS TO A SUBJECT MATTER WITHIN A DOMAIN
302
ANALYZING, USING A PROCESSING DEVICE, THE DOMAIN DATA
304
GENERATING, USING THE PROCESSING DEVICE, A KNOWLEDGE GRAPH OPERATION DATA BASED ON THE ANALYZING, WHEREIN THE KNOWLEDGE GRAPH OPERATION DATA COMPRISES AT LEAST ONE OF A CREATION DATA CONFIGURED FOR CREATING A KNOWLEDGE GRAPH DATA AND AN UPDATION DATA CONFIGURED FOR UPDATING THE KNOWLEDGE GRAPH DATA
306
EXECUTING, USING THE PROCESSING DEVICE, AT LEAST ONE OF THE CREATING AND THE UPDATING
308
STORING, USING A STORAGE DEVICE, THE KNOWLEDGE GRAPH OPERATION DATA ON A DECENTRALIZED DATABASE
310

Fig. 3

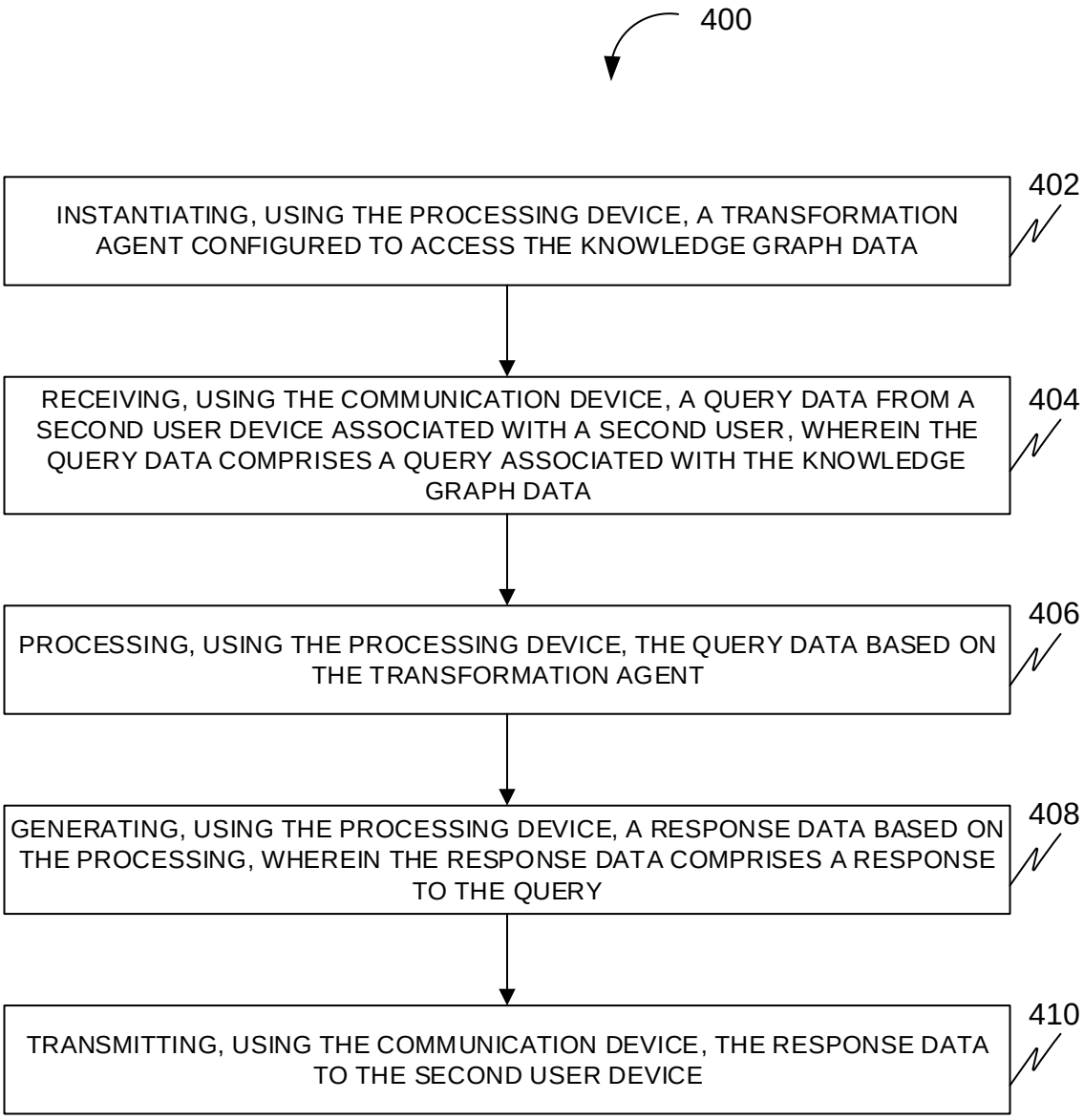

400
INSTANTIATING, USING THE PROCESSING DEVICE, A TRANSFORMATION AGENT CONFIGURED TO ACCESS THE KNOWLEDGE GRAPH DATA
402
RECEIVING, USING THE COMMUNICATION DEVICE, A QUERY DATA FROM A SECOND USER DEVICE ASSOCIATED WITH A SECOND USER, WHEREIN THE QUERY DATA COMPRISES A QUERY ASSOCIATED WITH THE KNOWLEDGE GRAPH DATA
404
PROCESSING, USING THE PROCESSING DEVICE, THE QUERY DATA BASED ON THE TRANSFORMATION AGENT
406
GENERATING, USING THE PROCESSING DEVICE, A RESPONSE DATA BASED ON THE PROCESSING, WHEREIN THE RESPONSE DATA COMPRISES A RESPONSE TO THE QUERY
408
TRANSMITTING, USING THE COMMUNICATION DEVICE, THE RESPONSE DATA TO THE SECOND USER DEVICE
410

Fig. 4

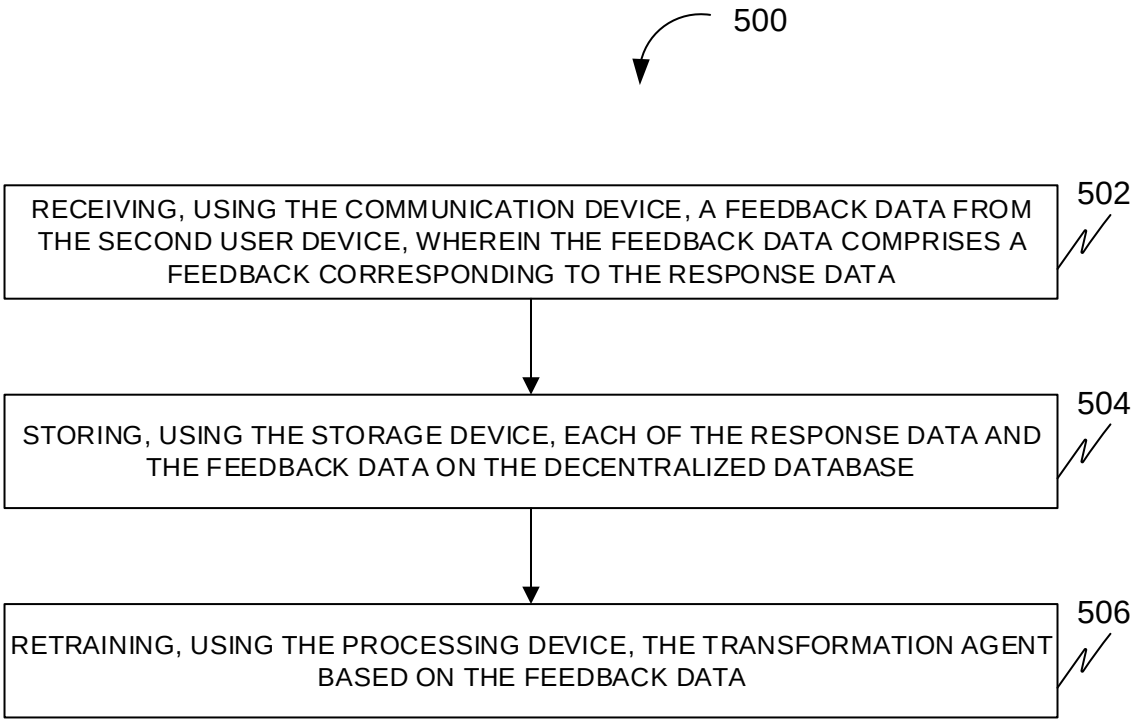

500
RECEIVING, USING THE COMMUNICATION DEVICE, A FEEDBACK DATA FROM THE SECOND USER DEVICE, WHEREIN THE FEEDBACK DATA COMPRISES A FEEDBACK CORRESPONDING TO THE RESPONSE DATA
502
STORING, USING THE STORAGE DEVICE, EACH OF THE RESPONSE DATA AND THE FEEDBACK DATA ON THE DECENTRALIZED DATABASE
504
RETRAINING, USING THE PROCESSING DEVICE, THE TRANSFORMATION AGENT BASED ON THE FEEDBACK DATA
506

Fig. 5

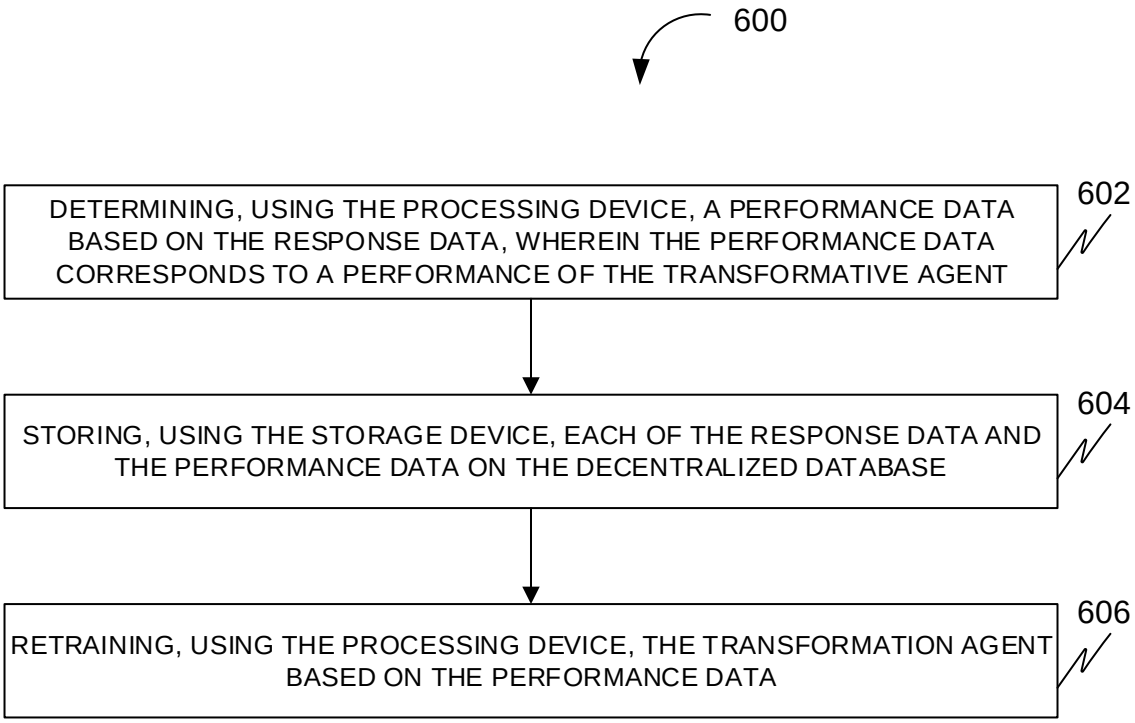

600
DETERMINING, USING THE PROCESSING DEVICE, A PERFORMANCE DATA BASED ON THE RESPONSE DATA, WHEREIN THE PERFORMANCE DATA CORRESPONDS TO A PERFORMANCE OF THE TRANSFORMATIVE AGENT
602
STORING, USING THE STORAGE DEVICE, EACH OF THE RESPONSE DATA AND THE PERFORMANCE DATA ON THE DECENTRALIZED DATABASE
604
RETRAINING, USING THE PROCESSING DEVICE, THE TRANSFORMATION AGENT BASED ON THE PERFORMANCE DATA
606

Fig. 6

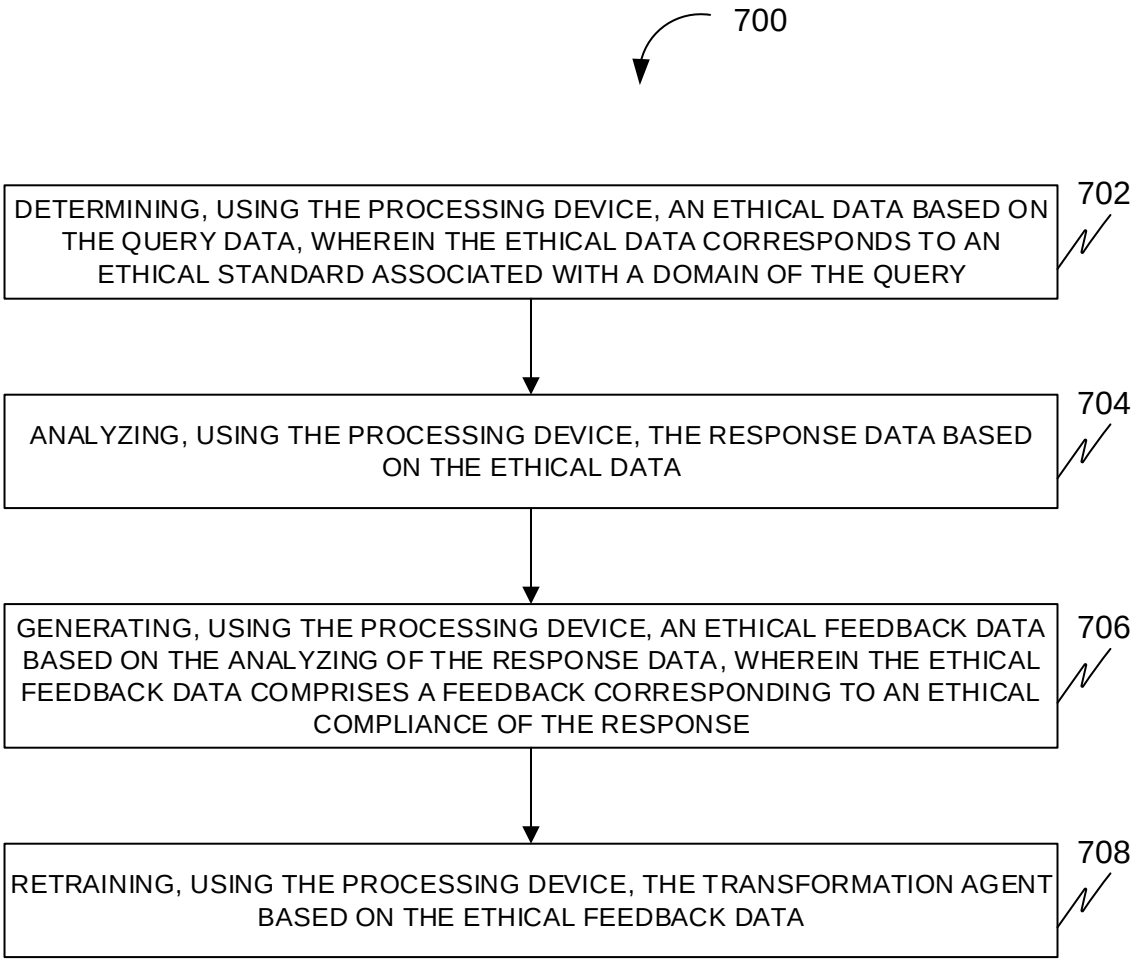

700
DETERMINING, USING THE PROCESSING DEVICE, AN ETHICAL DATA BASED ON THE QUERY DATA, WHEREIN THE ETHICAL DATA CORRESPONDS TO AN ETHICAL STANDARD ASSOCIATED WITH A DOMAIN OF THE QUERY
702
ANALYZING, USING THE PROCESSING DEVICE, THE RESPONSE DATA BASED ON THE ETHICAL DATA
704
GENERATING, USING THE PROCESSING DEVICE, AN ETHICAL FEEDBACK DATA BASED ON THE ANALYZING OF THE RESPONSE DATA, WHEREIN THE ETHICAL FEEDBACK DATA COMPRISES A FEEDBACK CORRESPONDING TO AN ETHICAL COMPLIANCE OF THE RESPONSE
706
RETRAINING, USING THE PROCESSING DEVICE, THE TRANSFORMATION AGENT BASED ON THE ETHICAL FEEDBACK DATA
708

Fig. 7

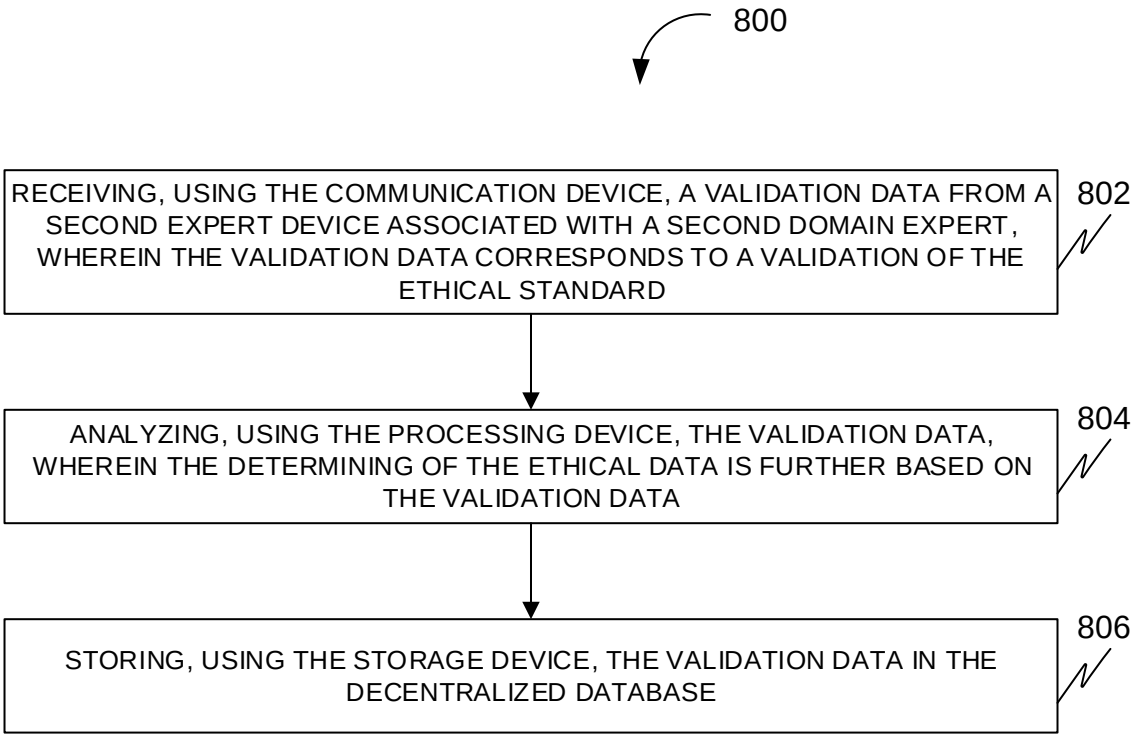

800
RECEIVING, USING THE COMMUNICATION DEVICE, A VALIDATION DATA FROM A SECOND EXPERT DEVICE ASSOCIATED WITH A SECOND DOMAIN EXPERT, WHEREIN THE VALIDATION DATA CORRESPONDS TO A VALIDATION OF THE ETHICAL STANDARD
802
ANALYZING, USING THE PROCESSING DEVICE, THE VALIDATION DATA, WHEREIN THE DETERMINING OF THE ETHICAL DATA IS FURTHER BASED ON THE VALIDATION DATA
804
STORING, USING THE STORAGE DEVICE, THE VALIDATION DATA IN THE DECENTRALIZED DATABASE
806

Fig. 8

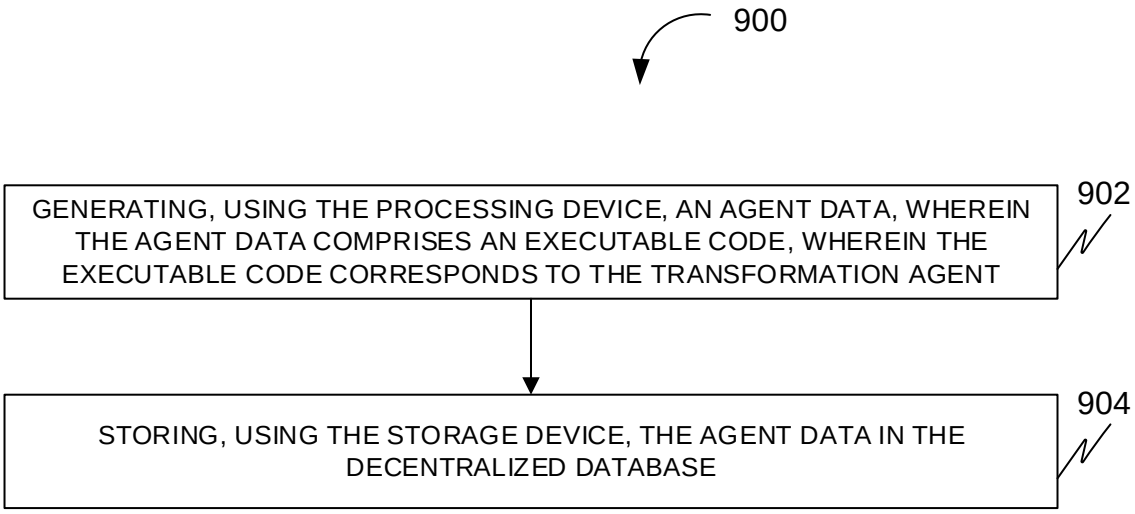

900
GENERATING, USING THE PROCESSING DEVICE, AN AGENT DATA, WHEREIN THE AGENT DATA COMPRISES AN EXECUTABLE CODE, WHEREIN THE EXECUTABLE CODE CORRESPONDS TO THE TRANSFORMATION AGENT
902
STORING, USING THE STORAGE DEVICE, THE AGENT DATA IN THE DECENTRALIZED DATABASE
904

Fig. 9

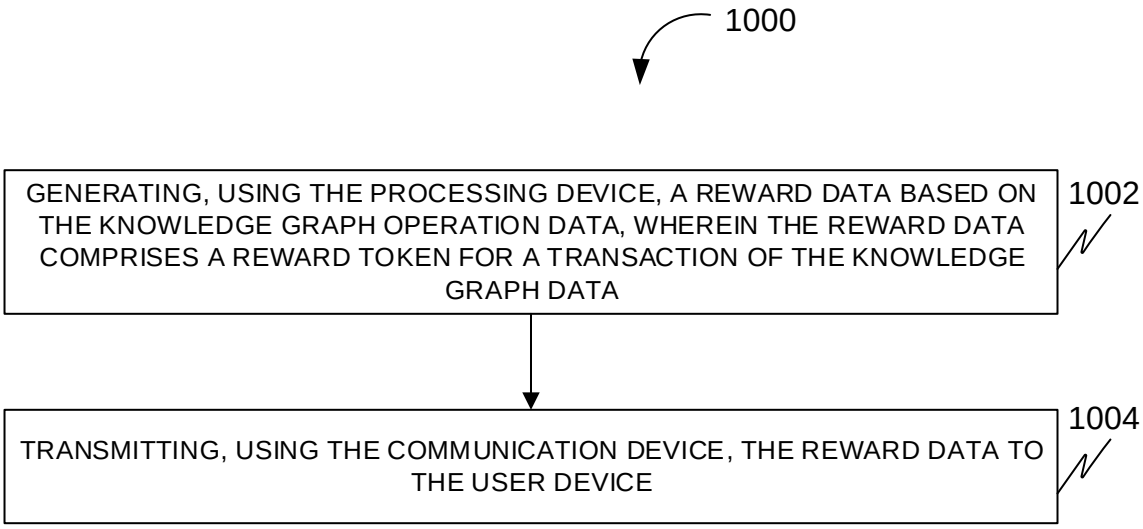

1000
GENERATING, USING THE PROCESSING DEVICE, A REWARD DATA BASED ON THE KNOWLEDGE GRAPH OPERATION DATA, WHEREIN THE REWARD DATA COMPRISES A REWARD TOKEN FOR A TRANSACTION OF THE KNOWLEDGE GRAPH DATA
1002
TRANSMITTING, USING THE COMMUNICATION DEVICE, THE REWARD DATA TO THE USER DEVICE
1004

Fig. 10

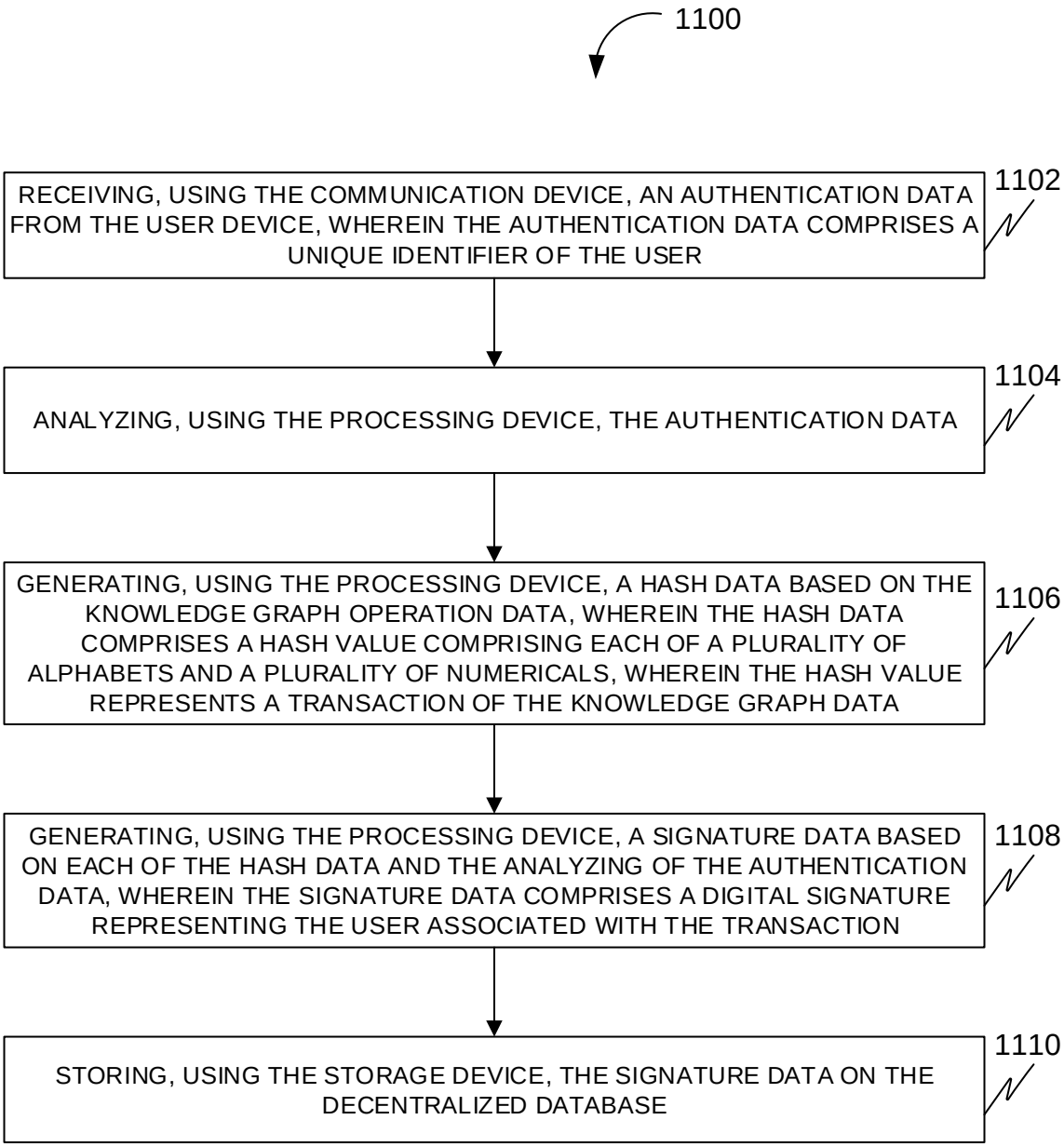

1100
RECEIVING, USING THE COMMUNICATION DEVICE, AN AUTHENTICATION DATA FROM THE USER DEVICE, WHEREIN THE AUTHENTICATION DATA COMPRISES A UNIQUE IDENTIFIER OF THE USER
1102
ANALYZING, USING THE PROCESSING DEVICE, THE AUTHENTICATION DATA
1104
GENERATING, USING THE PROCESSING DEVICE, A HASH DATA BASED ON THE KNOWLEDGE GRAPH OPERATION DATA, WHEREIN THE HASH DATA COMPRISES A HASH VALUE COMPRISING EACH OF A PLURALITY OF ALPHABETS AND A PLURALITY OF NUMERICALS, WHEREIN THE HASH VALUE REPRESENTS A TRANSACTION OF THE KNOWLEDGE GRAPH DATA
1106
GENERATING, USING THE PROCESSING DEVICE, A SIGNATURE DATA BASED ON EACH OF THE HASH DATA AND THE ANALYZING OF THE AUTHENTICATION DATA, WHEREIN THE SIGNATURE DATA COMPRISES A DIGITAL SIGNATURE REPRESENTING THE USER ASSOCIATED WITH THE TRANSACTION
1108
STORING, USING THE STORAGE DEVICE, THE SIGNATURE DATA ON THE DECENTRALIZED DATABASE
1110

Fig. 11

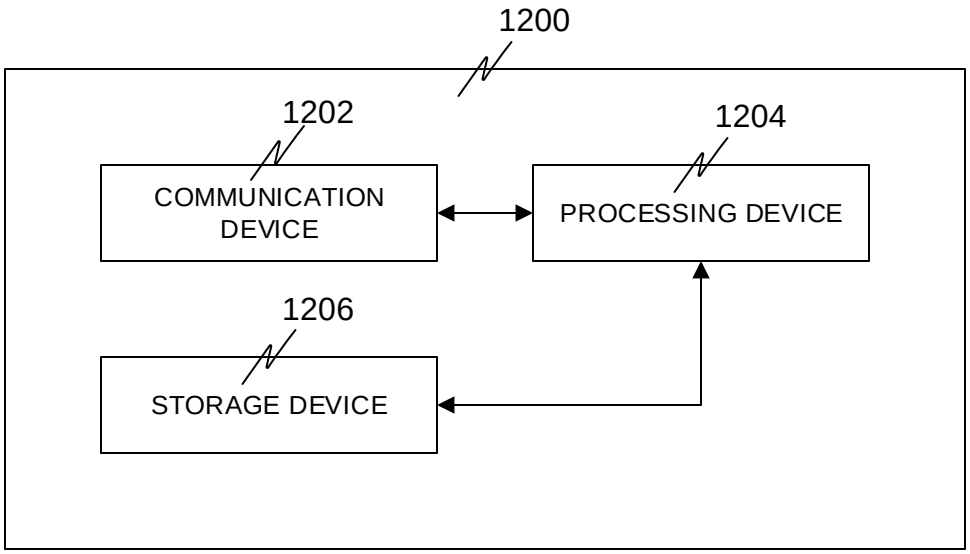

1200
1202
COMMUNICATION DEVICE
1204
PROCESSING DEVICE
1206
STORAGE DEVICE

Fig. 12

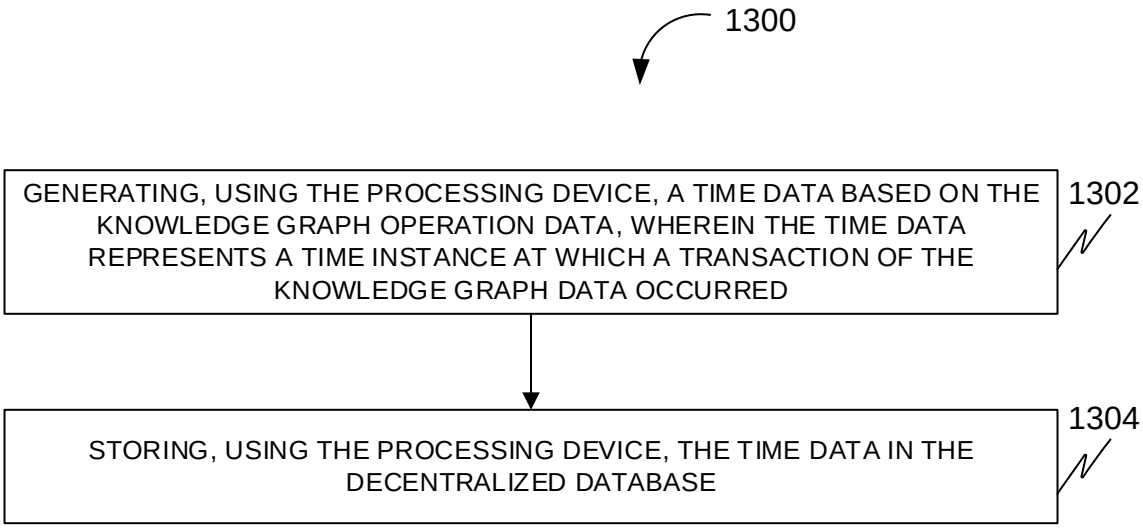

1300
GENERATING, USING THE PROCESSING DEVICE, A TIME DATA BASED ON THE KNOWLEDGE GRAPH OPERATION DATA, WHEREIN THE TIME DATA REPRESENTS A TIME INSTANCE AT WHICH A TRANSACTION OF THE KNOWLEDGE GRAPH DATA OCCURRED
1302
STORING, USING THE PROCESSING DEVICE, THE TIME DATA IN THE DECENTRALIZED DATABASE
1304

Fig. 13

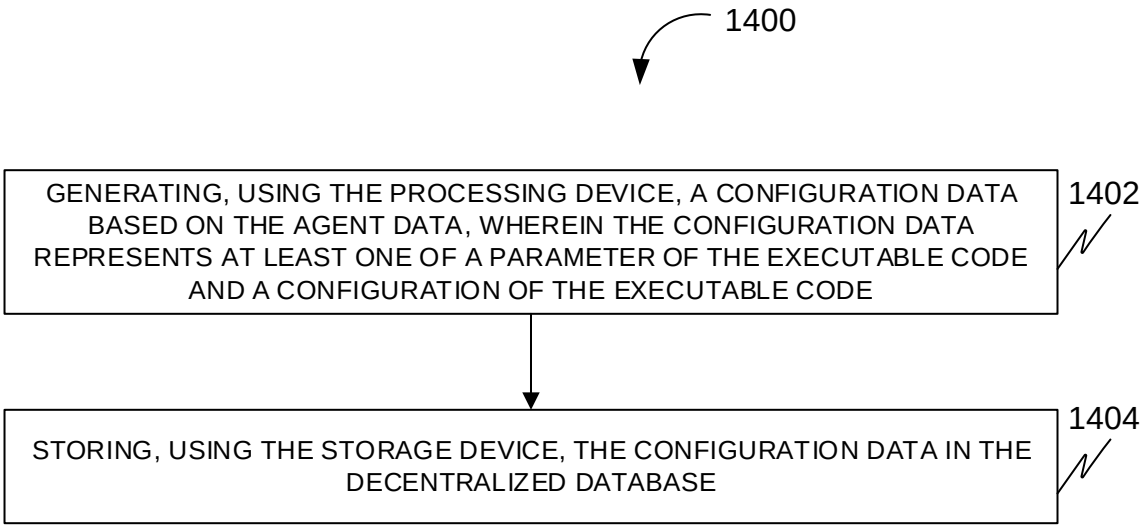

1400
GENERATING, USING THE PROCESSING DEVICE, A CONFIGURATION DATA BASED ON THE AGENT DATA, WHEREIN THE CONFIGURATION DATA REPRESENTS AT LEAST ONE OF A PARAMETER OF THE EXECUTABLE CODE AND A CONFIGURATION OF THE EXECUTABLE CODE
1402
STORING, USING THE STORAGE DEVICE, THE CONFIGURATION DATA IN THE DECENTRALIZED DATABASE
1404

Fig. 14

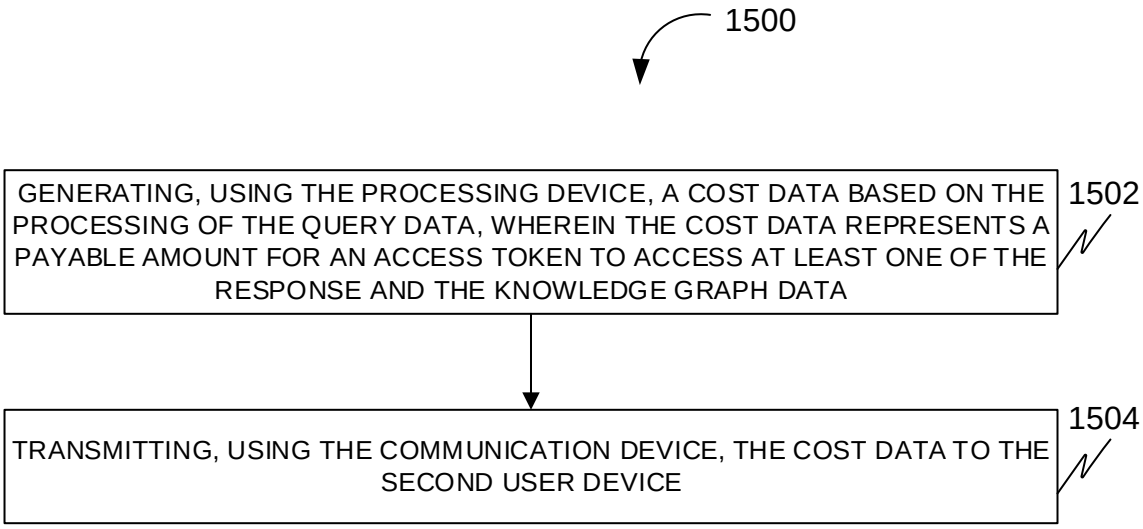

1500
GENERATING, USING THE PROCESSING DEVICE, A COST DATA BASED ON THE PROCESSING OF THE QUERY DATA, WHEREIN THE COST DATA REPRESENTS A PAYABLE AMOUNT FOR AN ACCESS TOKEN TO ACCESS AT LEAST ONE OF THE RESPONSE AND THE KNOWLEDGE GRAPH DATA
1502
TRANSMITTING, USING THE COMMUNICATION DEVICE, THE COST DATA TO THE SECOND USER DEVICE
1504

Fig. 15

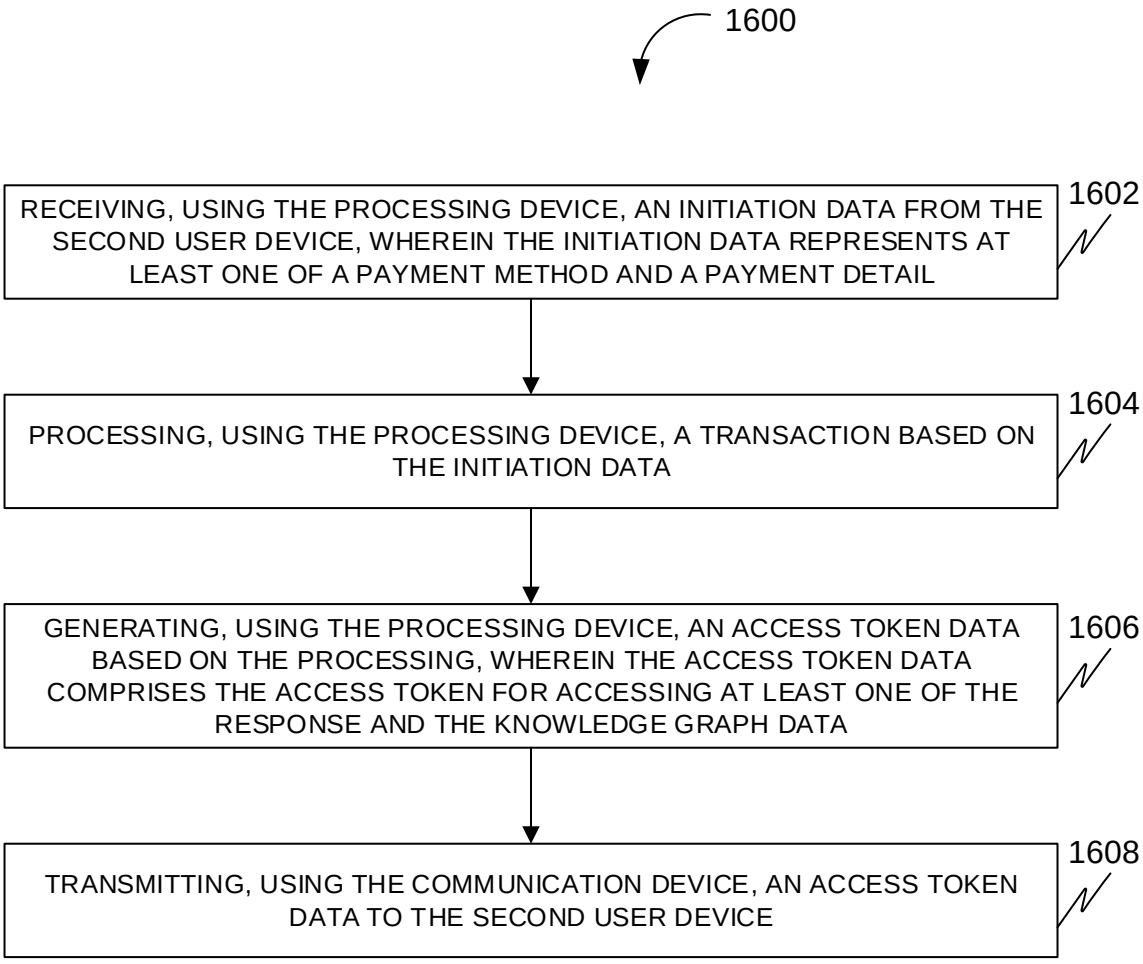

1600
RECEIVING, USING THE PROCESSING DEVICE, AN INITIATION DATA FROM THE SECOND USER DEVICE, WHEREIN THE INITIATION DATA REPRESENTS AT LEAST ONE OF A PAYMENT METHOD AND A PAYMENT DETAIL
1602
PROCESSING, USING THE PROCESSING DEVICE, A TRANSACTION BASED ON THE INITIATION DATA
1604
GENERATING, USING THE PROCESSING DEVICE, AN ACCESS TOKEN DATA BASED ON THE PROCESSING, WHEREIN THE ACCESS TOKEN DATA COMPRISES THE ACCESS TOKEN FOR ACCESSING AT LEAST ONE OF THE RESPONSE AND THE KNOWLEDGE GRAPH DATA
1606
TRANSMITTING, USING THE COMMUNICATION DEVICE, AN ACCESS TOKEN DATA TO THE SECOND USER DEVICE
1608

Fig. 16

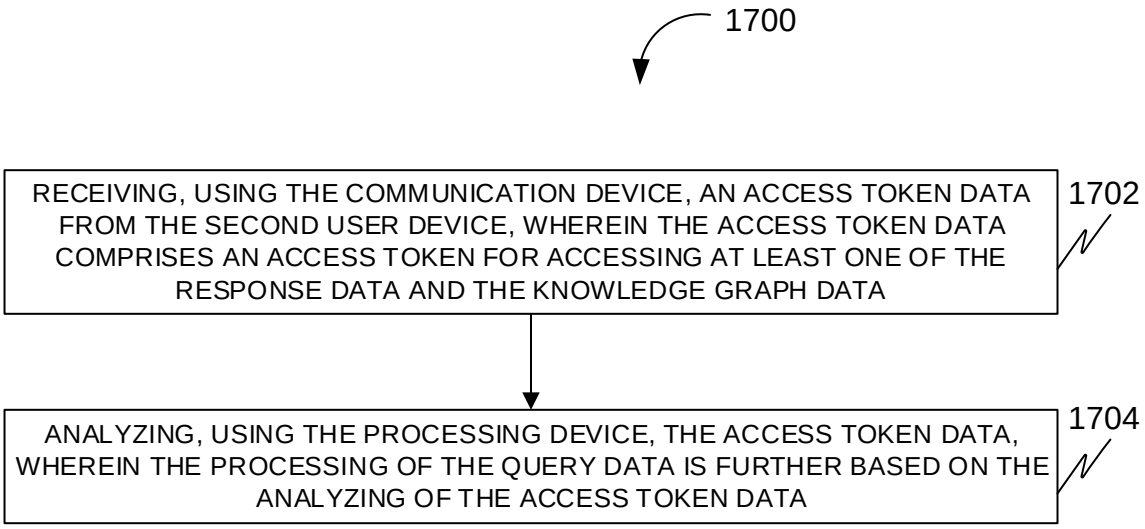

1700
RECEIVING, USING THE COMMUNICATION DEVICE, AN ACCESS TOKEN DATA FROM THE SECOND USER DEVICE, WHEREIN THE ACCESS TOKEN DATA COMPRISES AN ACCESS TOKEN FOR ACCESSING AT LEAST ONE OF THE RESPONSE DATA AND THE KNOWLEDGE GRAPH DATA
1702
ANALYZING, USING THE PROCESSING DEVICE, THE ACCESS TOKEN DATA, WHEREIN THE PROCESSING OF THE QUERY DATA IS FURTHER BASED ON THE ANALYZING OF THE ACCESS TOKEN DATA
1704

Fig. 17

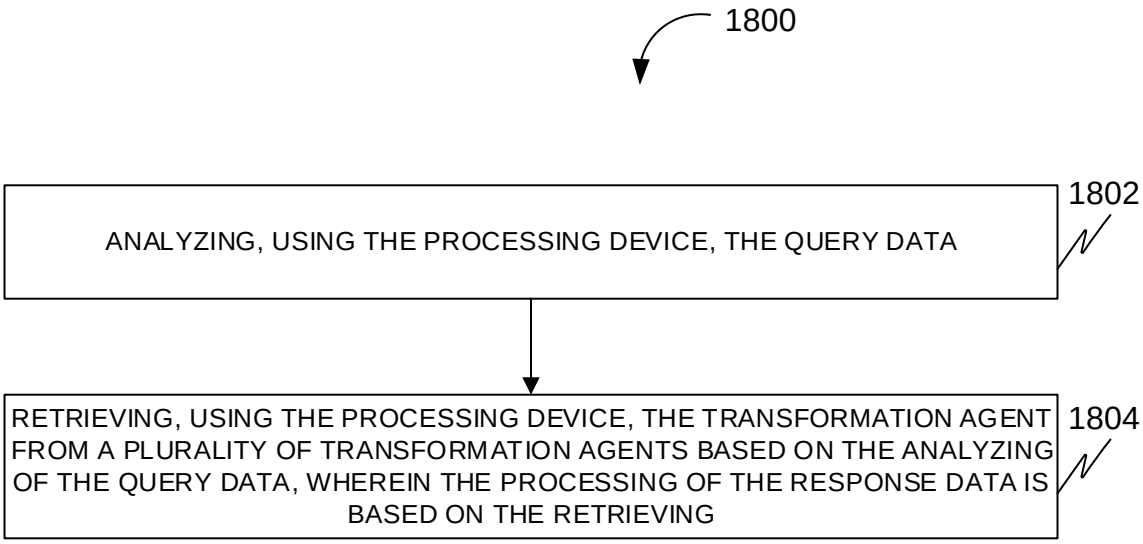

1800
ANALYZING, USING THE PROCESSING DEVICE, THE QUERY DATA
1802
RETRIEVING, USING THE PROCESSING DEVICE, THE TRANSFORMATION AGENT FROM A PLURALITY OF TRANSFORMATION AGENTS BASED ON THE ANALYZING OF THE QUERY DATA, WHEREIN THE PROCESSING OF THE RESPONSE DATA IS BASED ON THE RETRIEVING
1804

Fig. 18

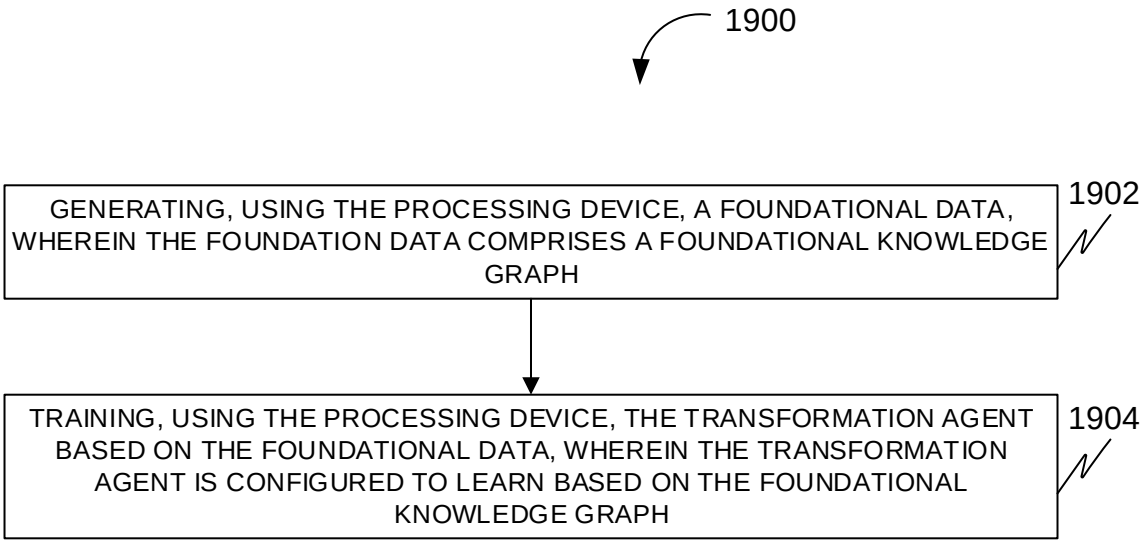

1900
GENERATING, USING THE PROCESSING DEVICE, A FOUNDATIONAL DATA, WHEREIN THE FOUNDATION DATA COMPRISES A FOUNDATIONAL KNOWLEDGE GRAPH
1902
TRAINING, USING THE PROCESSING DEVICE, THE TRANSFORMATION AGENT BASED ON THE FOUNDATIONAL DATA, WHEREIN THE TRANSFORMATION AGENT IS CONFIGURED TO LEARN BASED ON THE FOUNDATIONAL KNOWLEDGE GRAPH
1904

Fig. 19

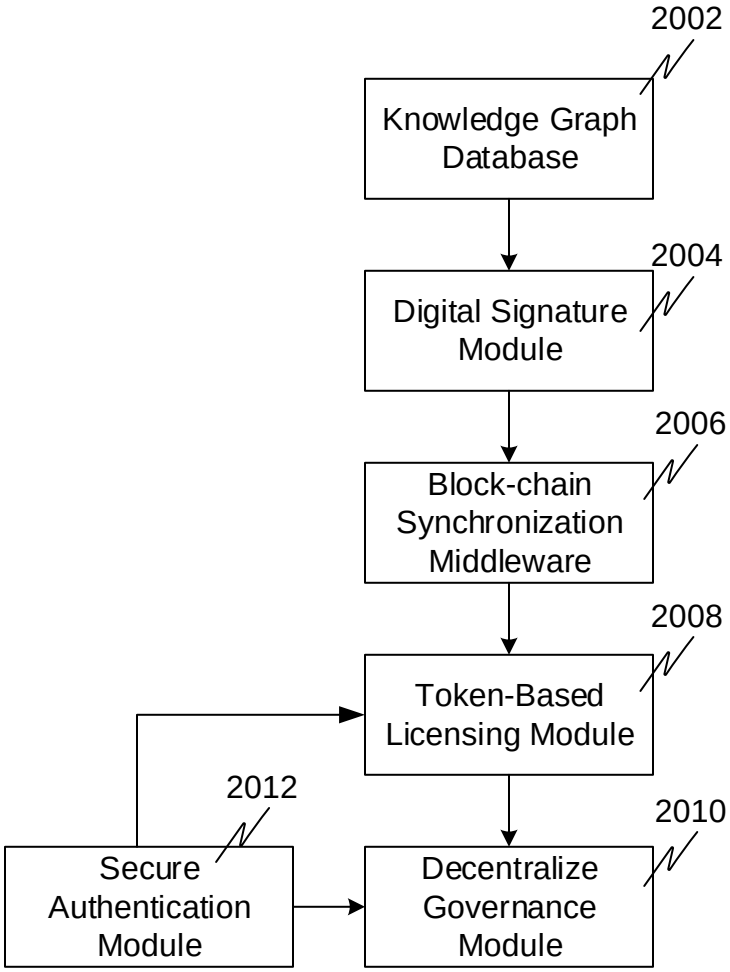

2002
Knowledge Graph Database
2004
Digital Signature Module
2006
Block-chain Synchronization Middleware
2008
Token-Based Licensing Module
2012
Secure Authentication Module
2010
Decentralize Governance Module

Fig. 20

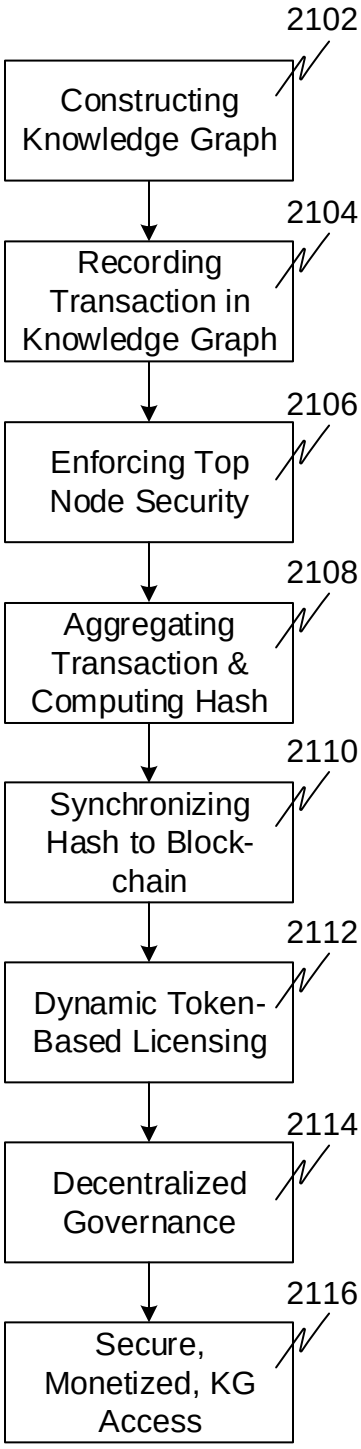

2102
Constructing Knowledge Graph
2104
Recording Transaction in Knowledge Graph
2106
Enforcing Top Node Security
2108
Aggregating Transaction & Computing Hash
2110
Synchronizing Hash to Block-chain
2112
Dynamic Token-Based Licensing
2114
Decentralized Governance
2116
Secure, Monetized, KG Access

Fig. 21

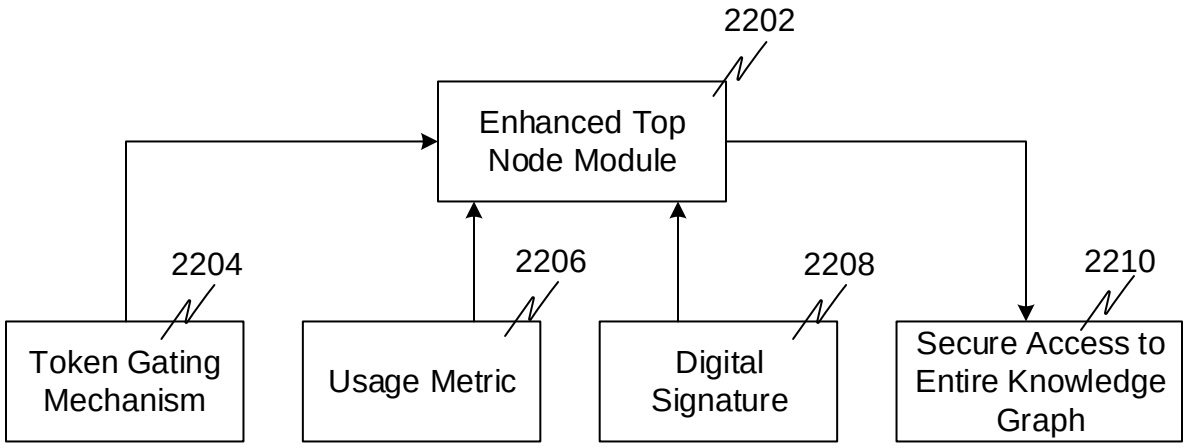

2202
Enhanced Top Node Module
2204
Token Gating Mechanism
2206
Usage Metric
2208
Digital Signature
2210
Secure Access to Entire Knowledge Graph

Fig. 22

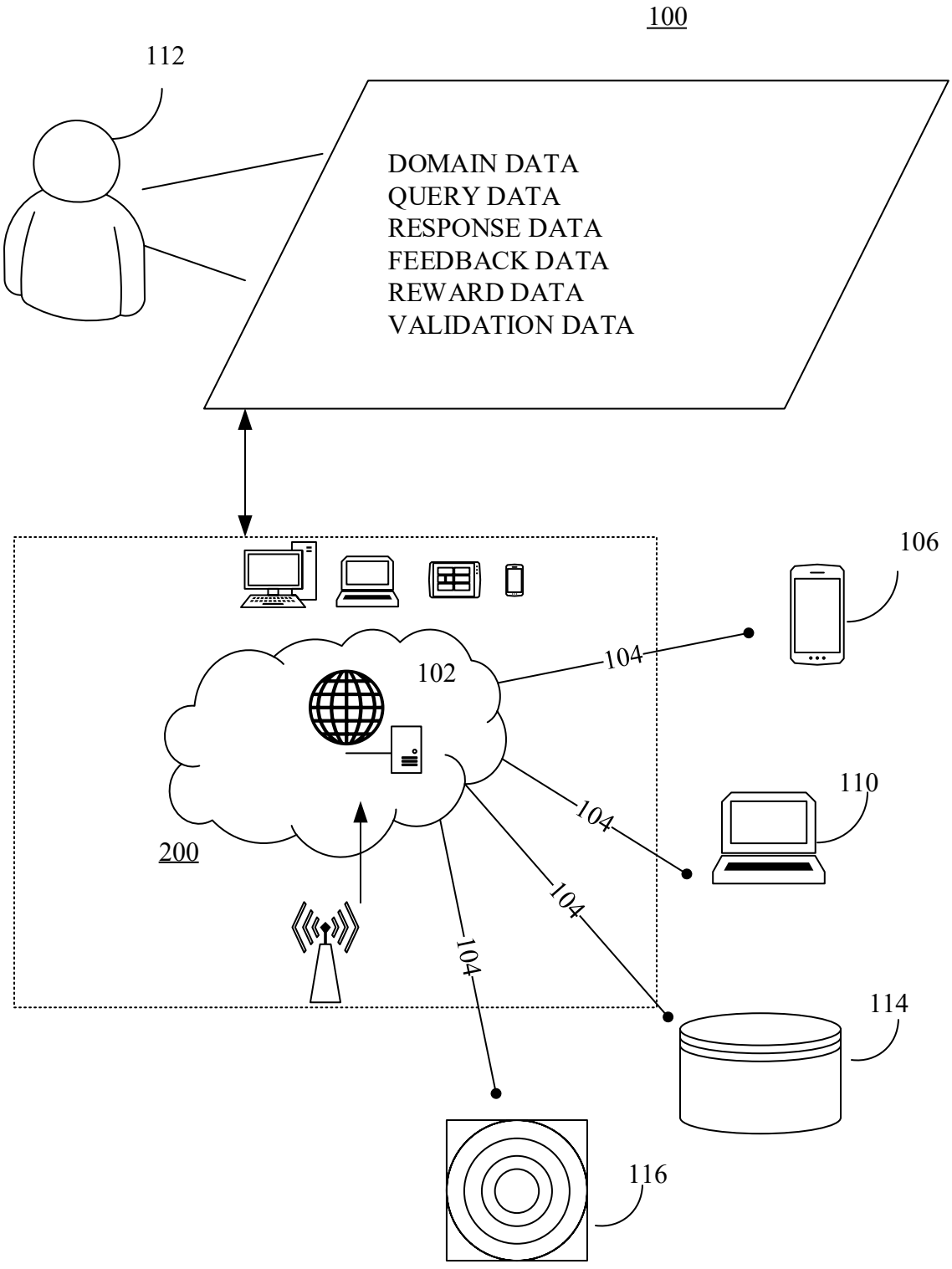

100
112
DOMAIN DATA
QUERY DATA
RESPONSE DATA
FEEDBACK DATA
REWARD DATA
VALIDATION DATA
106
102
104
110
200
104
104
104
114
116

Fig. 1

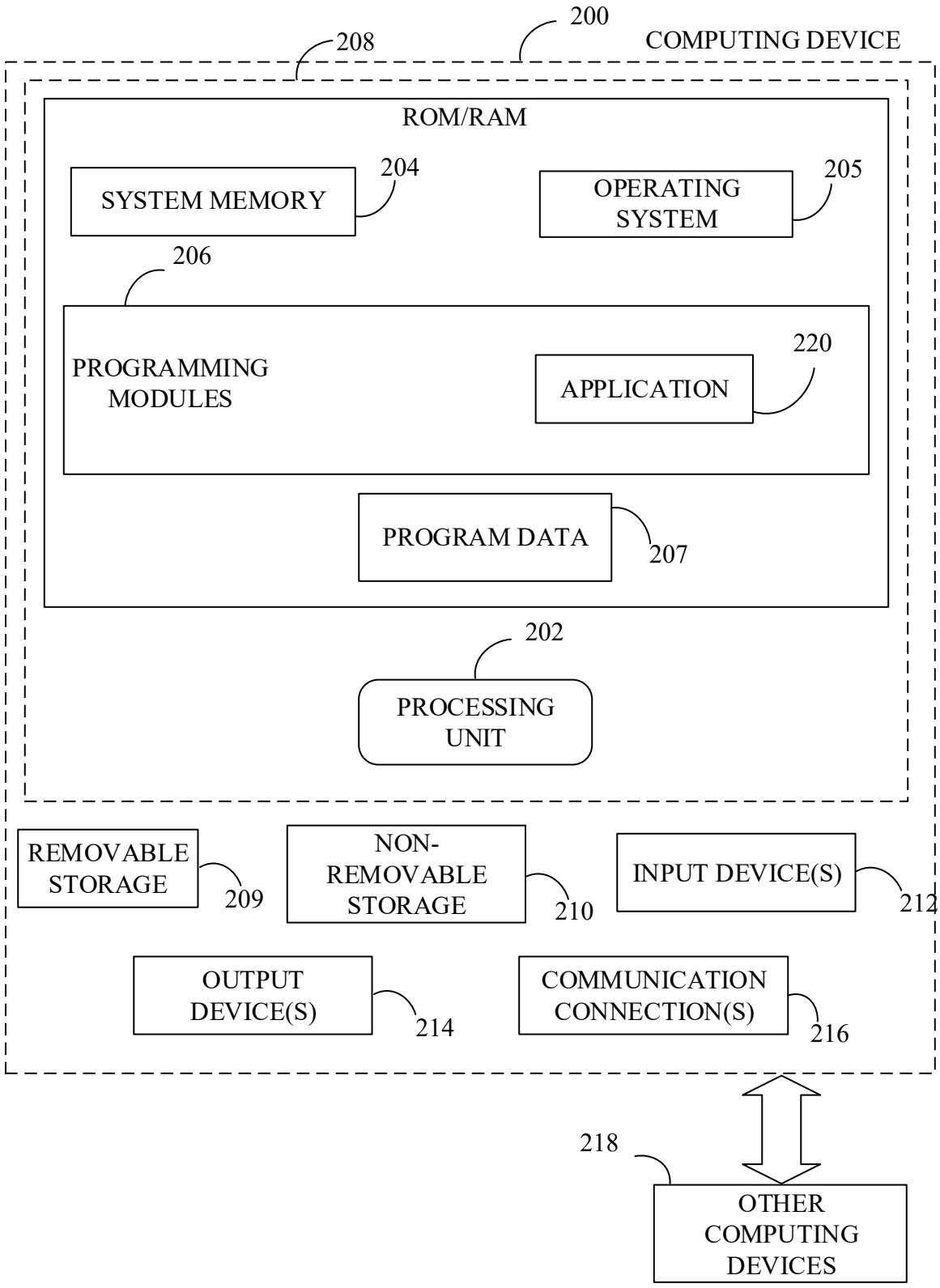

200
COMPUTING DEVICE
208
ROM/RAM
SYSTEM MEMORY
204
OPERATING SYSTEM
205
206
PROGRAMMING MODULES
220
APPLICATION
PROGRAM DATA
207
202
PROCESSING UNIT
REMOVABLE STORAGE
209
NON-REMOVABLE STORAGE
210
INPUT DEVICE(S)
212
OUTPUT DEVICE(S)
214
COMMUNICATION CONNECTION(S)
216
218
OTHER COMPUTING DEVICES

Fig. 2

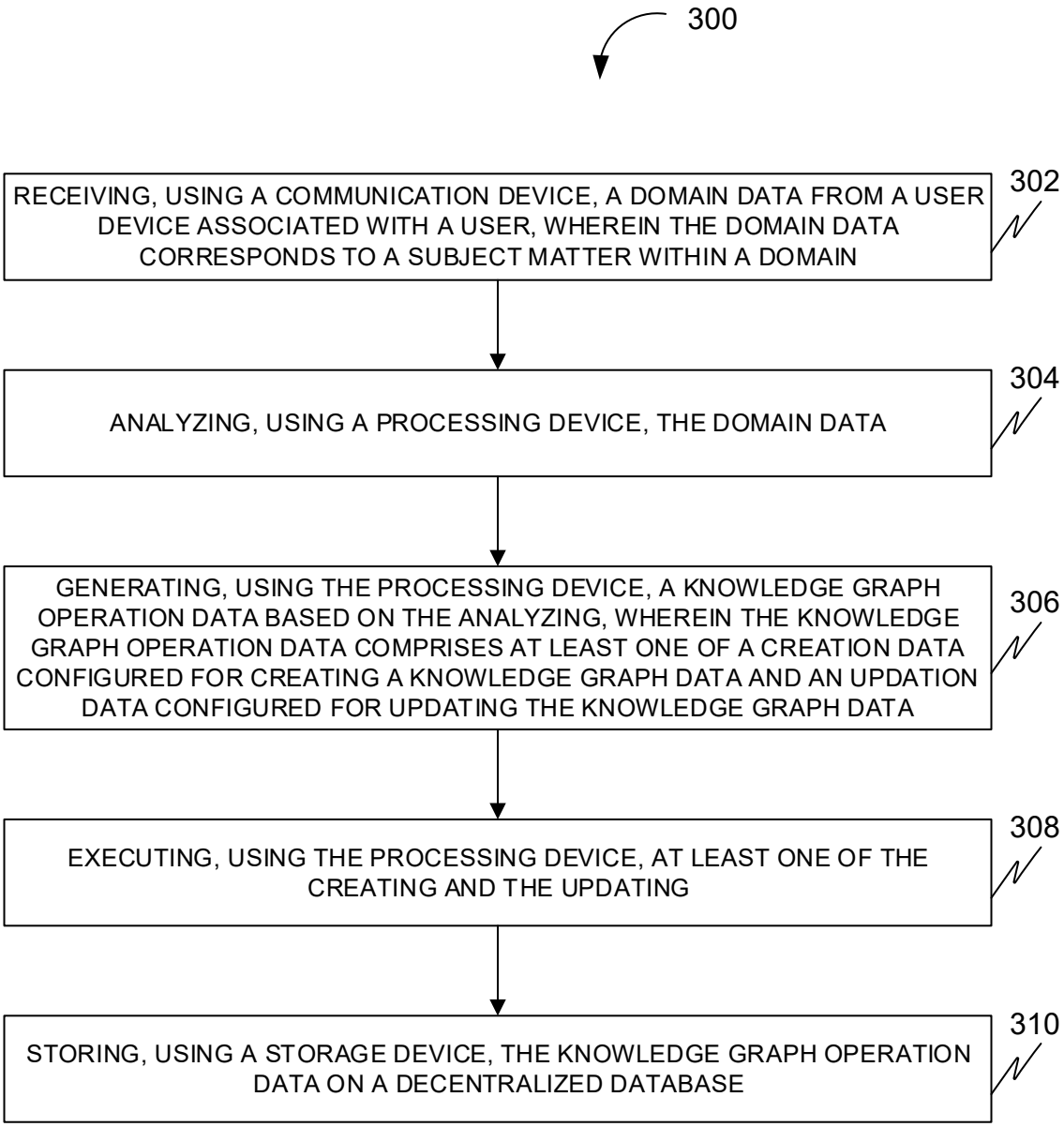

300
RECEIVING, USING A COMMUNICATION DEVICE, A DOMAIN DATA FROM A USER DEVICE ASSOCIATED WITH A USER, WHEREIN THE DOMAIN DATA CORRESPONDS TO A SUBJECT MATTER WITHIN A DOMAIN
302
ANALYZING, USING A PROCESSING DEVICE, THE DOMAIN DATA
304
GENERATING, USING THE PROCESSING DEVICE, A KNOWLEDGE GRAPH OPERATION DATA BASED ON THE ANALYZING, WHEREIN THE KNOWLEDGE GRAPH OPERATION DATA COMPRISES AT LEAST ONE OF A CREATION DATA CONFIGURED FOR CREATING A KNOWLEDGE GRAPH DATA AND AN UPDATION DATA CONFIGURED FOR UPDATING THE KNOWLEDGE GRAPH DATA
306
EXECUTING, USING THE PROCESSING DEVICE, AT LEAST ONE OF THE CREATING AND THE UPDATING
308
STORING, USING A STORAGE DEVICE, THE KNOWLEDGE GRAPH OPERATION DATA ON A DECENTRALIZED DATABASE
310

Fig. 3

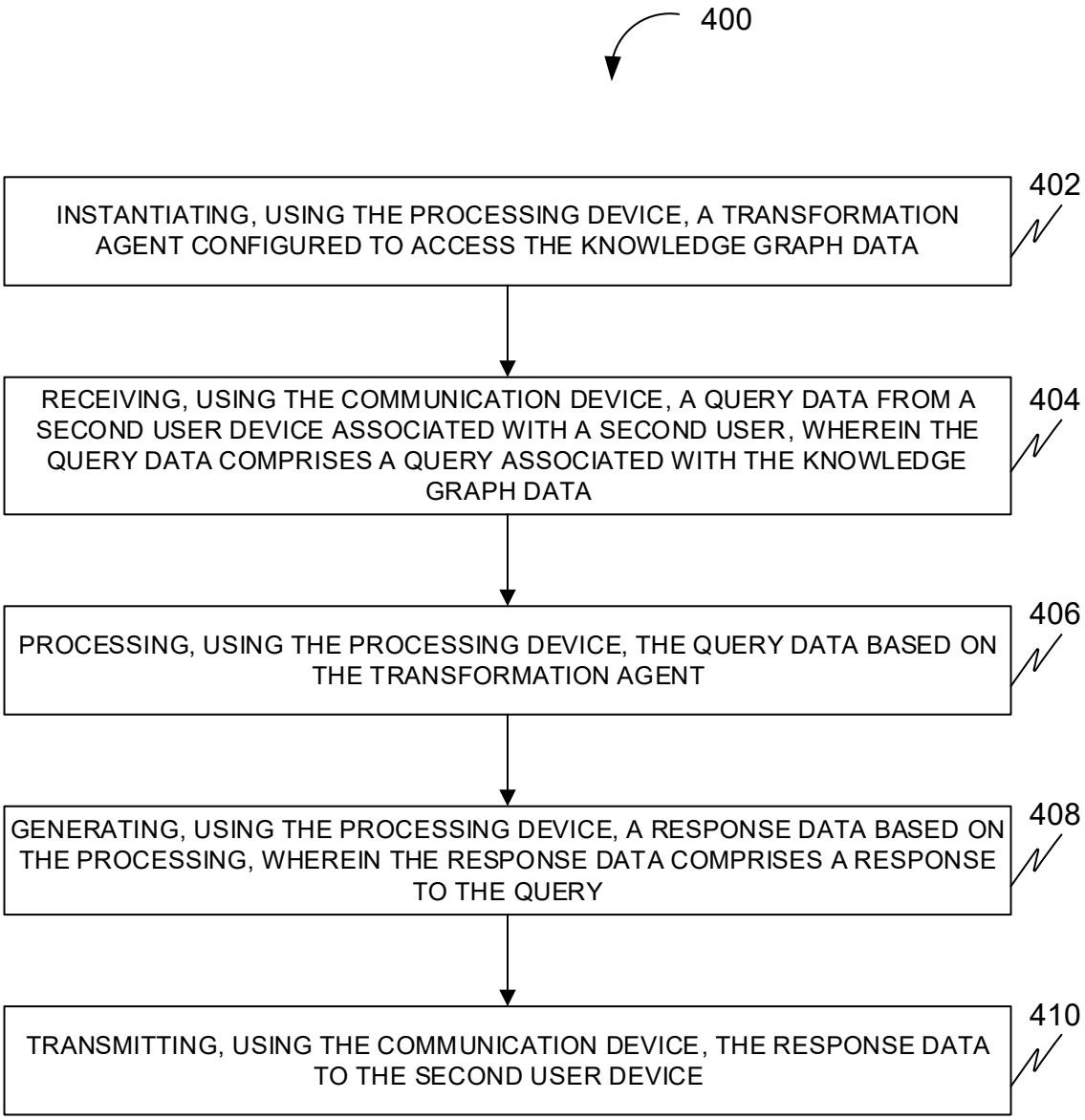

400
INSTANTIATING, USING THE PROCESSING DEVICE, A TRANSFORMATION AGENT CONFIGURED TO ACCESS THE KNOWLEDGE GRAPH DATA
402
RECEIVING, USING THE COMMUNICATION DEVICE, A QUERY DATA FROM A SECOND USER DEVICE ASSOCIATED WITH A SECOND USER, WHEREIN THE QUERY DATA COMPRISES A QUERY ASSOCIATED WITH THE KNOWLEDGE GRAPH DATA
404
PROCESSING, USING THE PROCESSING DEVICE, THE QUERY DATA BASED ON THE TRANSFORMATION AGENT
406
GENERATING, USING THE PROCESSING DEVICE, A RESPONSE DATA BASED ON THE PROCESSING, WHEREIN THE RESPONSE DATA COMPRISES A RESPONSE TO THE QUERY
408
TRANSMITTING, USING THE COMMUNICATION DEVICE, THE RESPONSE DATA TO THE SECOND USER DEVICE
410

Fig. 4

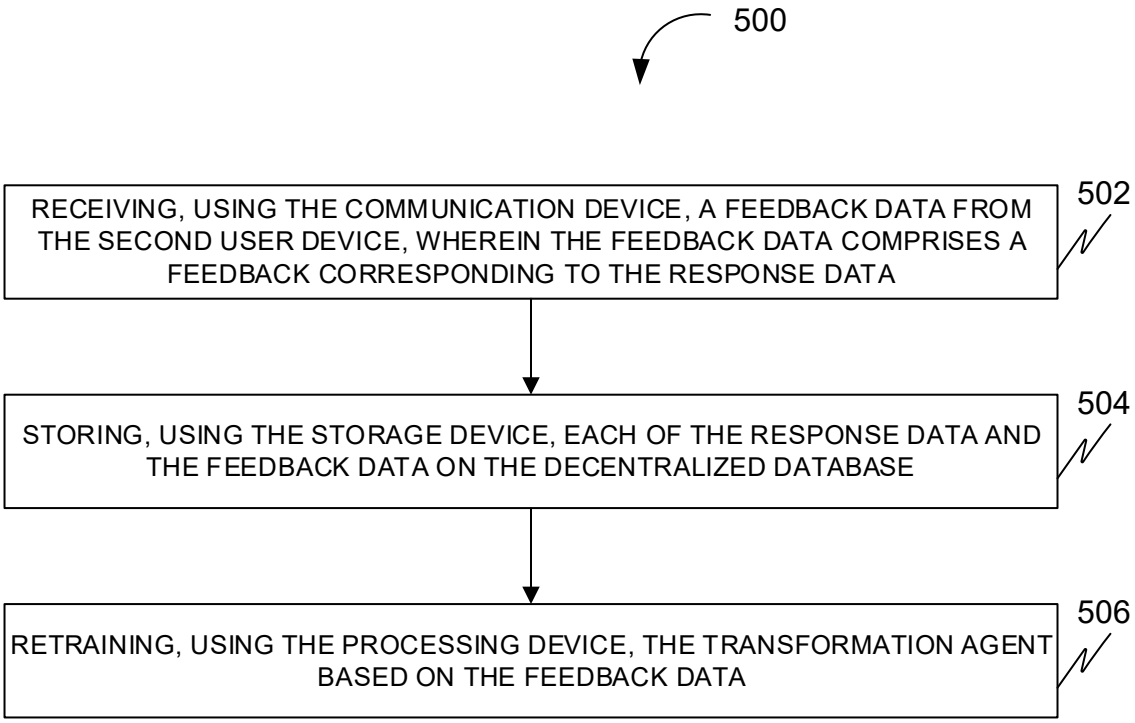

500
RECEIVING, USING THE COMMUNICATION DEVICE, A FEEDBACK DATA FROM THE SECOND USER DEVICE, WHEREIN THE FEEDBACK DATA COMPRISES A FEEDBACK CORRESPONDING TO THE RESPONSE DATA
502
STORING, USING THE STORAGE DEVICE, EACH OF THE RESPONSE DATA AND THE FEEDBACK DATA ON THE DECENTRALIZED DATABASE
504
RETRAINING, USING THE PROCESSING DEVICE, THE TRANSFORMATION AGENT BASED ON THE FEEDBACK DATA
506

Fig. 5

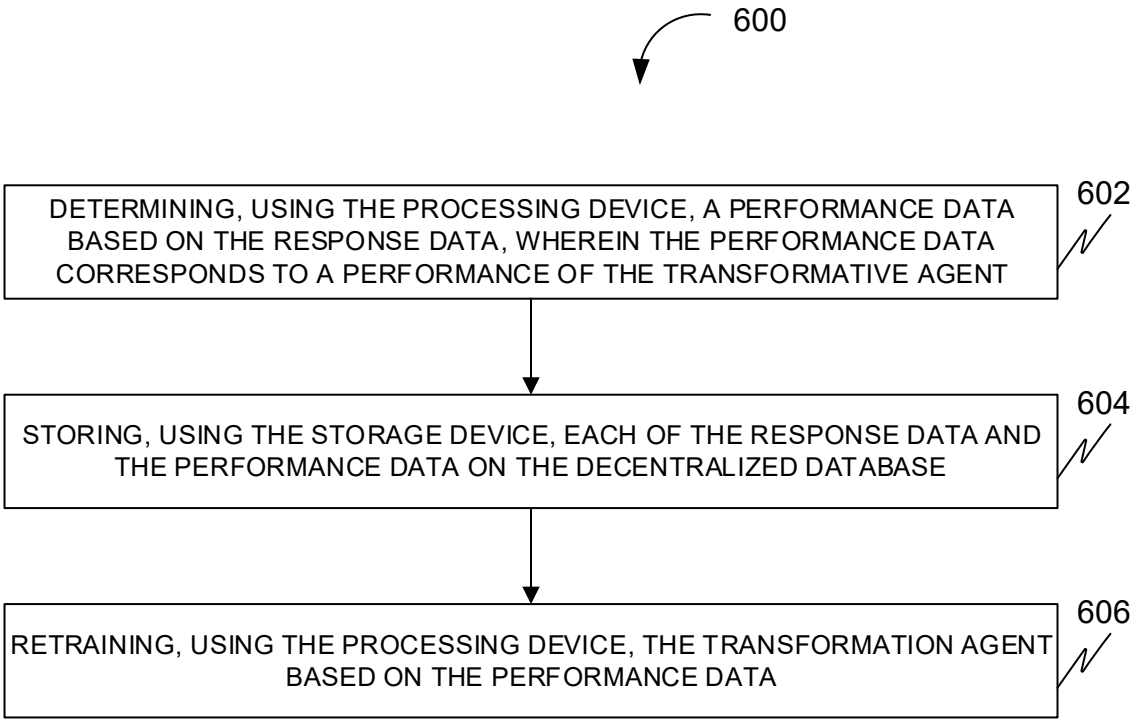

600
DETERMINING, USING THE PROCESSING DEVICE, A PERFORMANCE DATA BASED ON THE RESPONSE DATA, WHEREIN THE PERFORMANCE DATA CORRESPONDS TO A PERFORMANCE OF THE TRANSFORMATIVE AGENT
602
STORING, USING THE STORAGE DEVICE, EACH OF THE RESPONSE DATA AND THE PERFORMANCE DATA ON THE DECENTRALIZED DATABASE
604
RETRAINING, USING THE PROCESSING DEVICE, THE TRANSFORMATION AGENT BASED ON THE PERFORMANCE DATA
606

Fig. 6

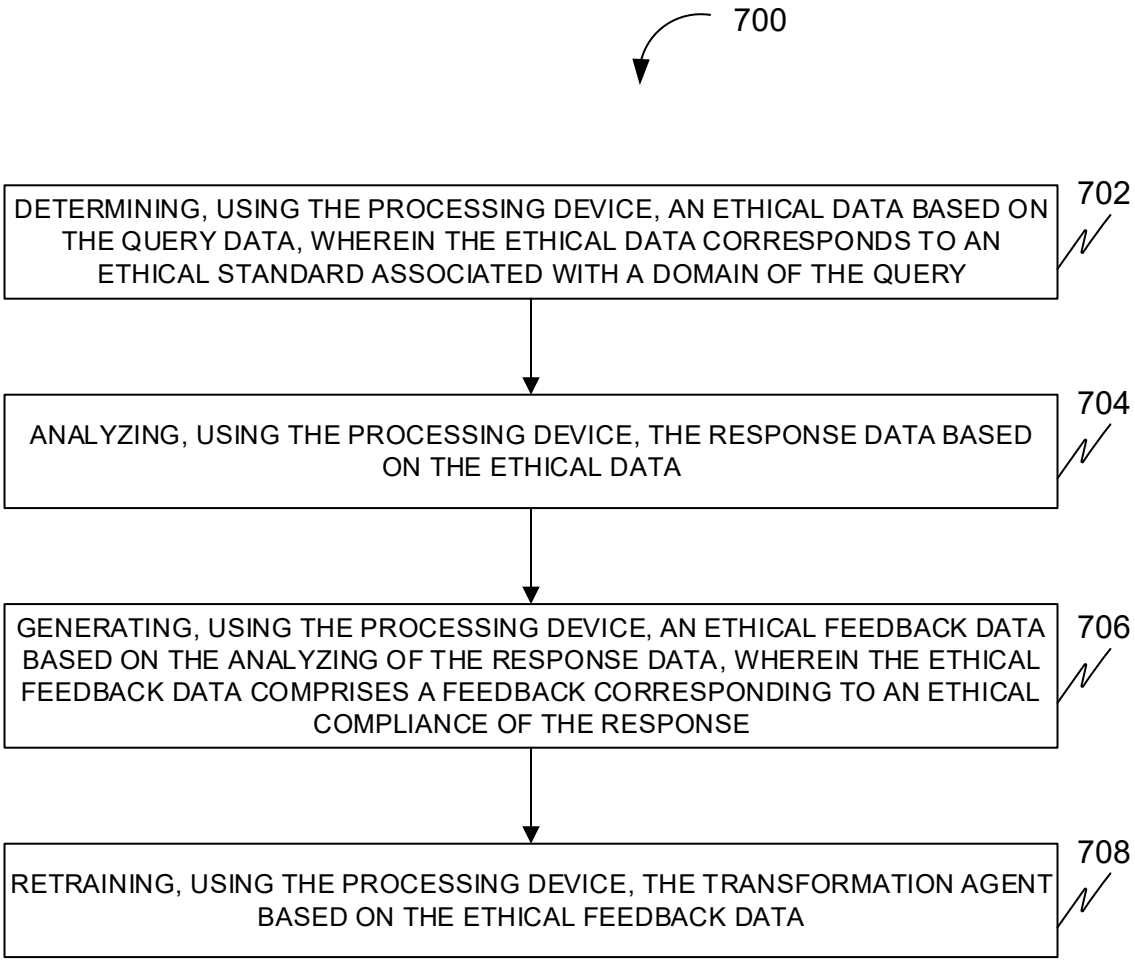

700
DETERMINING, USING THE PROCESSING DEVICE, AN ETHICAL DATA BASED ON THE QUERY DATA, WHEREIN THE ETHICAL DATA CORRESPONDS TO AN ETHICAL STANDARD ASSOCIATED WITH A DOMAIN OF THE QUERY
702
ANALYZING, USING THE PROCESSING DEVICE, THE RESPONSE DATA BASED ON THE ETHICAL DATA
704
GENERATING, USING THE PROCESSING DEVICE, AN ETHICAL FEEDBACK DATA BASED ON THE ANALYZING OF THE RESPONSE DATA, WHEREIN THE ETHICAL FEEDBACK DATA COMPRISES A FEEDBACK CORRESPONDING TO AN ETHICAL COMPLIANCE OF THE RESPONSE
706
RETRAINING, USING THE PROCESSING DEVICE, THE TRANSFORMATION AGENT BASED ON THE ETHICAL FEEDBACK DATA
708

Fig. 7

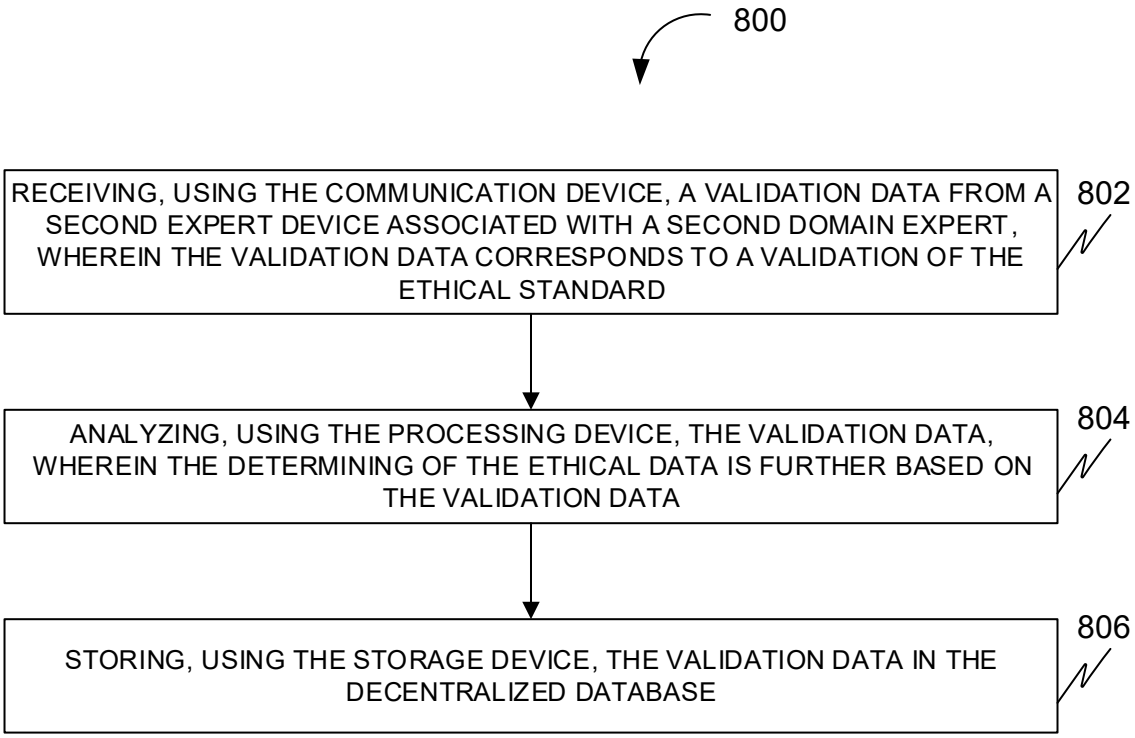

800
RECEIVING, USING THE COMMUNICATION DEVICE, A VALIDATION DATA FROM A SECOND EXPERT DEVICE ASSOCIATED WITH A SECOND DOMAIN EXPERT, WHEREIN THE VALIDATION DATA CORRESPONDS TO A VALIDATION OF THE ETHICAL STANDARD
802
ANALYZING, USING THE PROCESSING DEVICE, THE VALIDATION DATA, WHEREIN THE DETERMINING OF THE ETHICAL DATA IS FURTHER BASED ON THE VALIDATION DATA
804
STORING, USING THE STORAGE DEVICE, THE VALIDATION DATA IN THE DECENTRALIZED DATABASE
806

Fig. 8

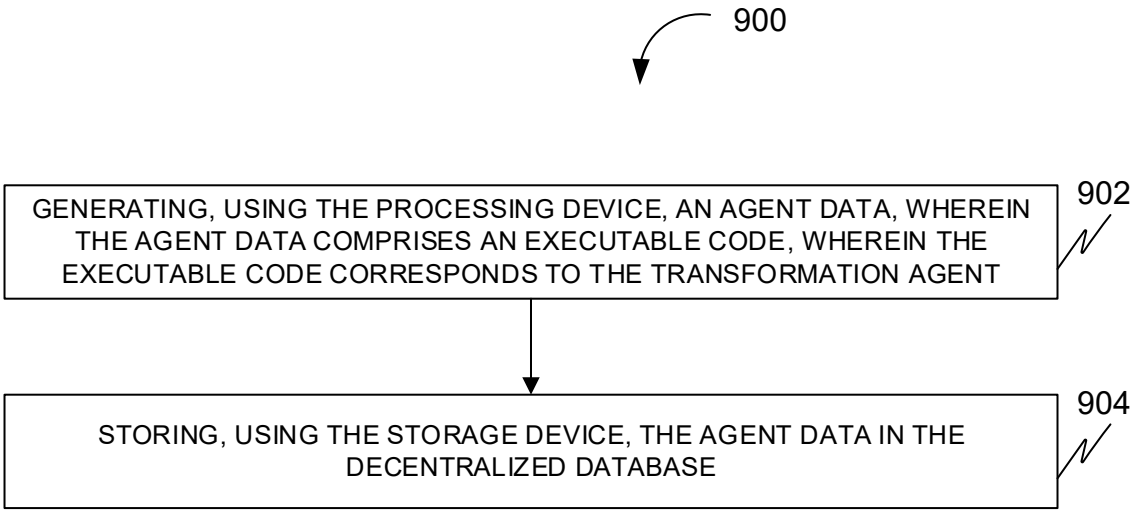

900
GENERATING, USING THE PROCESSING DEVICE, AN AGENT DATA, WHEREIN THE AGENT DATA COMPRISES AN EXECUTABLE CODE, WHEREIN THE EXECUTABLE CODE CORRESPONDS TO THE TRANSFORMATION AGENT
902
STORING, USING THE STORAGE DEVICE, THE AGENT DATA IN THE DECENTRALIZED DATABASE
904

Fig. 9

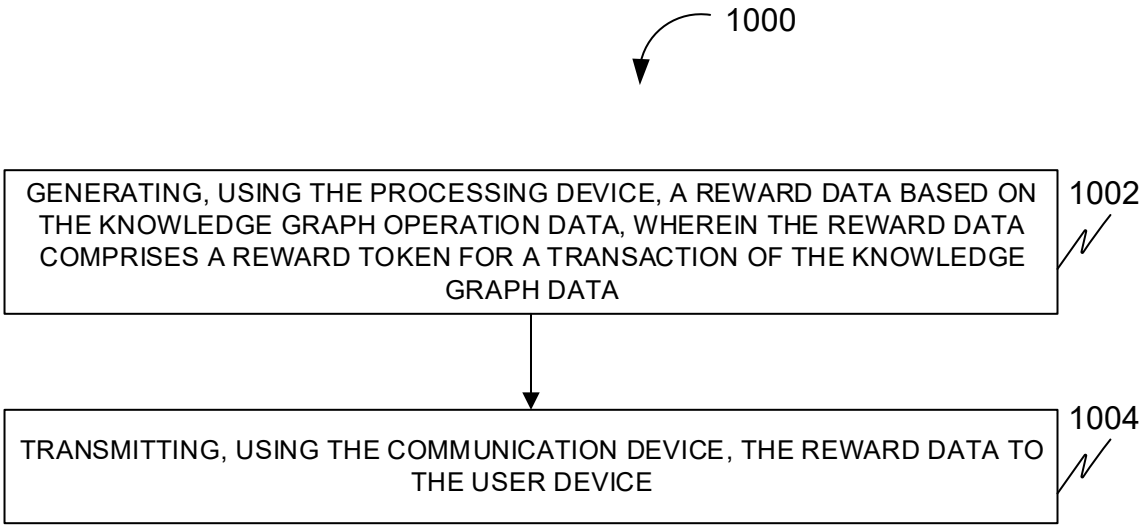

1000
GENERATING, USING THE PROCESSING DEVICE, A REWARD DATA BASED ON THE KNOWLEDGE GRAPH OPERATION DATA, WHEREIN THE REWARD DATA COMPRISES A REWARD TOKEN FOR A TRANSACTION OF THE KNOWLEDGE GRAPH DATA
1002
TRANSMITTING, USING THE COMMUNICATION DEVICE, THE REWARD DATA TO THE USER DEVICE
1004

Fig. 10

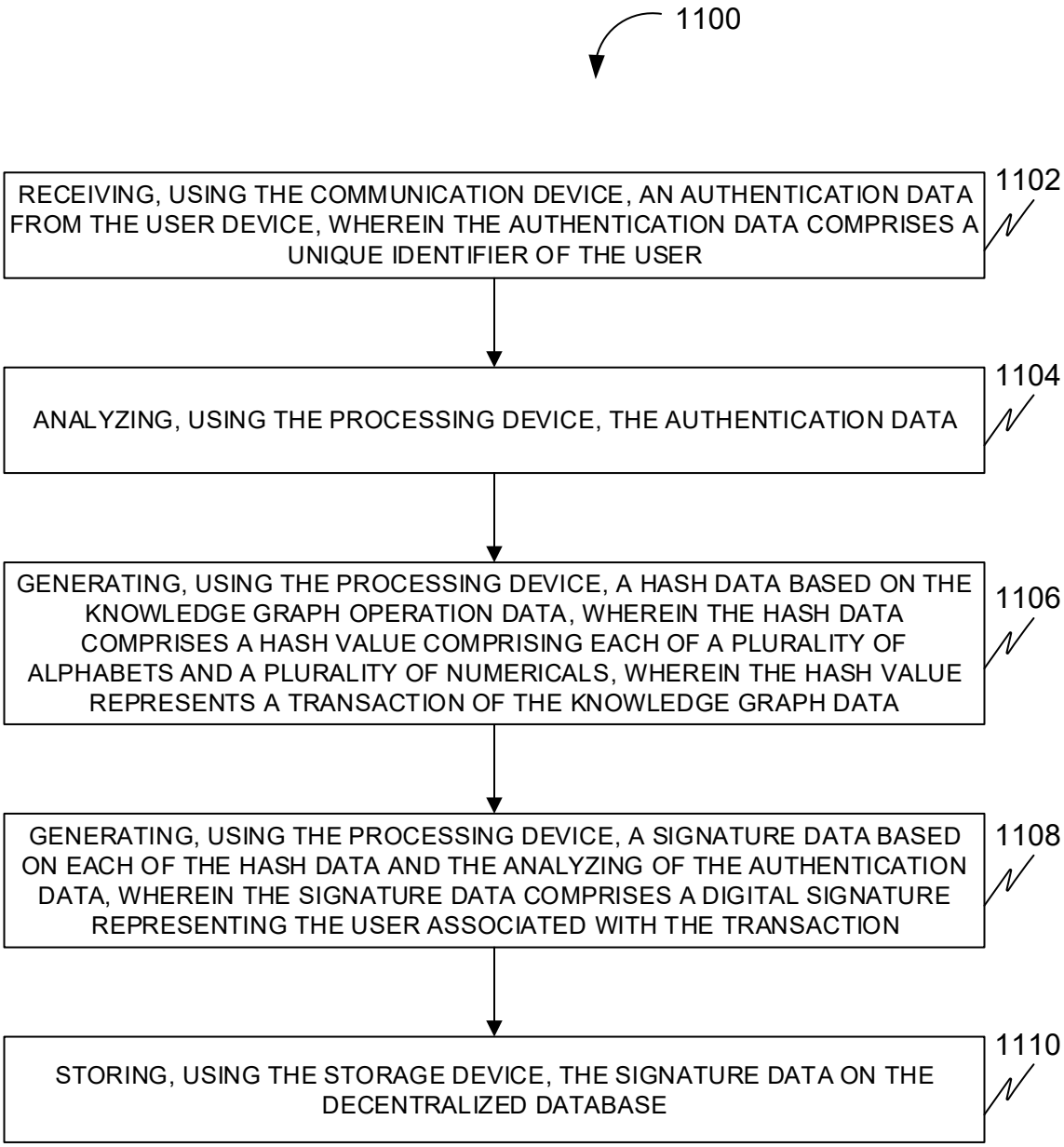

1100
RECEIVING, USING THE COMMUNICATION DEVICE, AN AUTHENTICATION DATA FROM THE USER DEVICE, WHEREIN THE AUTHENTICATION DATA COMPRISES A UNIQUE IDENTIFIER OF THE USER
1102
ANALYZING, USING THE PROCESSING DEVICE, THE AUTHENTICATION DATA
1104
GENERATING, USING THE PROCESSING DEVICE, A HASH DATA BASED ON THE KNOWLEDGE GRAPH OPERATION DATA, WHEREIN THE HASH DATA COMPRISES A HASH VALUE COMPRISING EACH OF A PLURALITY OF ALPHABETS AND A PLURALITY OF NUMERICALS, WHEREIN THE HASH VALUE REPRESENTS A TRANSACTION OF THE KNOWLEDGE GRAPH DATA
1106
GENERATING, USING THE PROCESSING DEVICE, A SIGNATURE DATA BASED ON EACH OF THE HASH DATA AND THE ANALYZING OF THE AUTHENTICATION DATA, WHEREIN THE SIGNATURE DATA COMPRISES A DIGITAL SIGNATURE REPRESENTING THE USER ASSOCIATED WITH THE TRANSACTION
1108
STORING, USING THE STORAGE DEVICE, THE SIGNATURE DATA ON THE DECENTRALIZED DATABASE
1110

Fig. 11

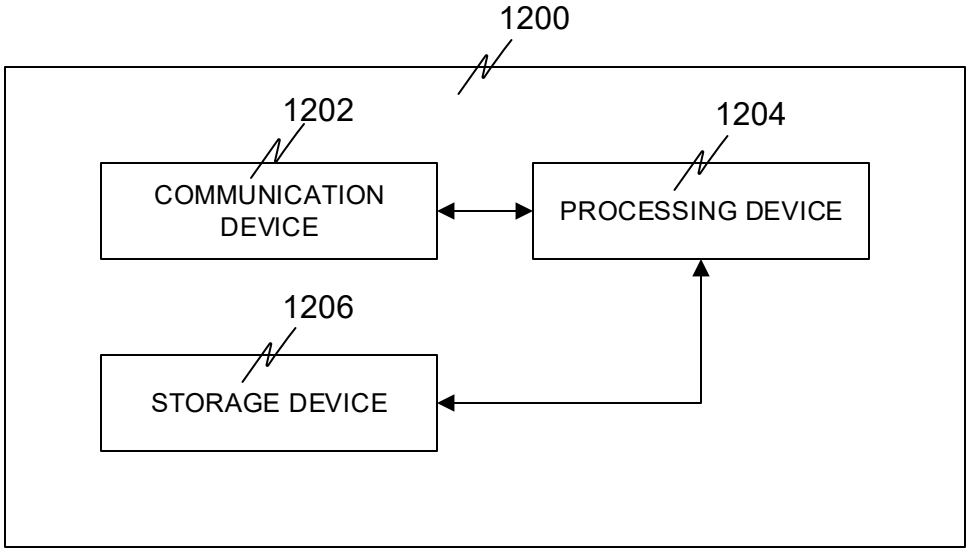

1200
1202
COMMUNICATION DEVICE
1204
PROCESSING DEVICE
1206
STORAGE DEVICE

Fig. 12

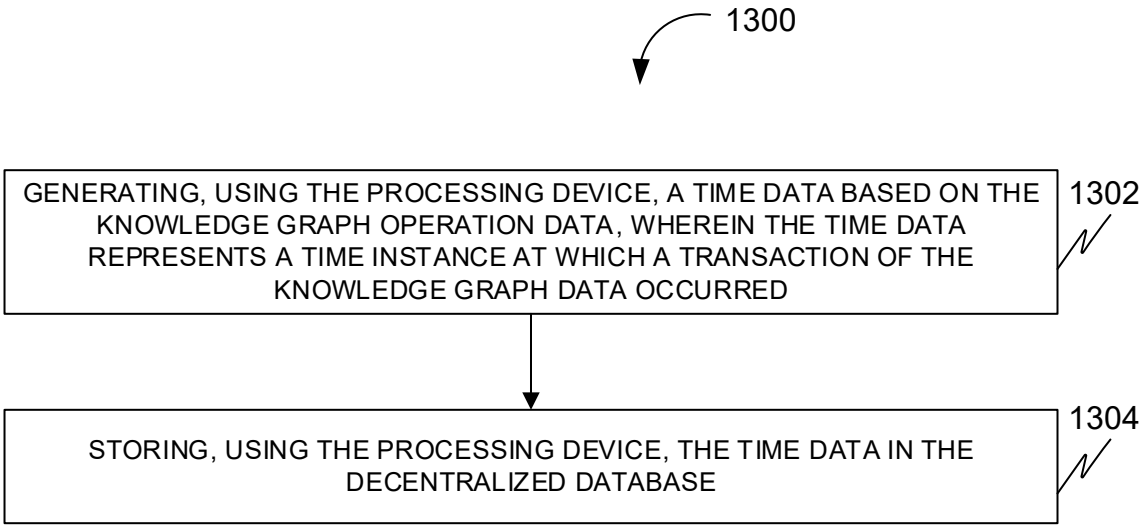

1300
GENERATING, USING THE PROCESSING DEVICE, A TIME DATA BASED ON THE KNOWLEDGE GRAPH OPERATION DATA, WHEREIN THE TIME DATA REPRESENTS A TIME INSTANCE AT WHICH A TRANSACTION OF THE KNOWLEDGE GRAPH DATA OCCURRED
1302
STORING, USING THE PROCESSING DEVICE, THE TIME DATA IN THE DECENTRALIZED DATABASE
1304

Fig. 13

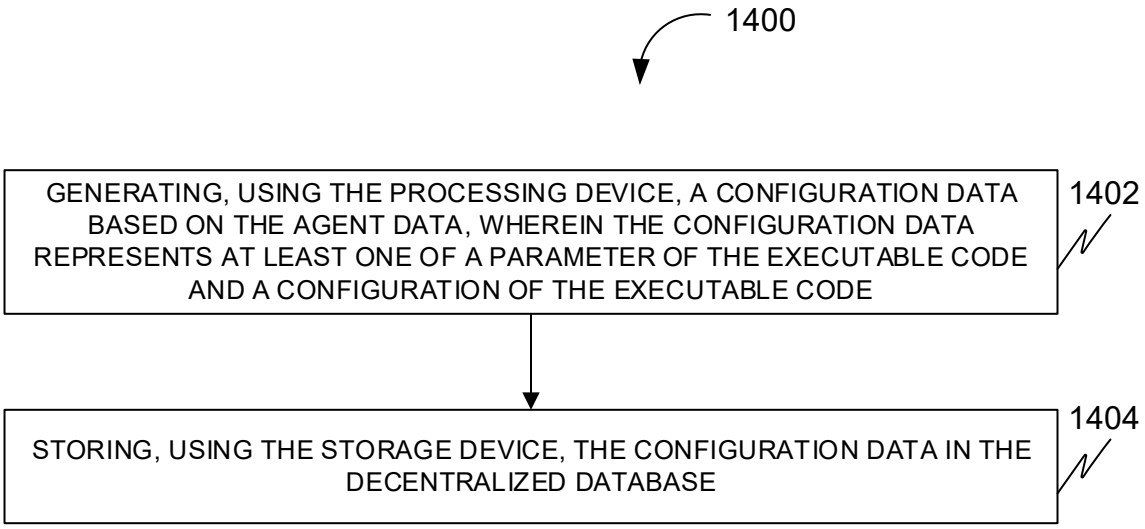

1400
GENERATING, USING THE PROCESSING DEVICE, A CONFIGURATION DATA BASED ON THE AGENT DATA, WHEREIN THE CONFIGURATION DATA REPRESENTS AT LEAST ONE OF A PARAMETER OF THE EXECUTABLE CODE AND A CONFIGURATION OF THE EXECUTABLE CODE
1402
STORING, USING THE STORAGE DEVICE, THE CONFIGURATION DATA IN THE DECENTRALIZED DATABASE
1404

Fig. 14

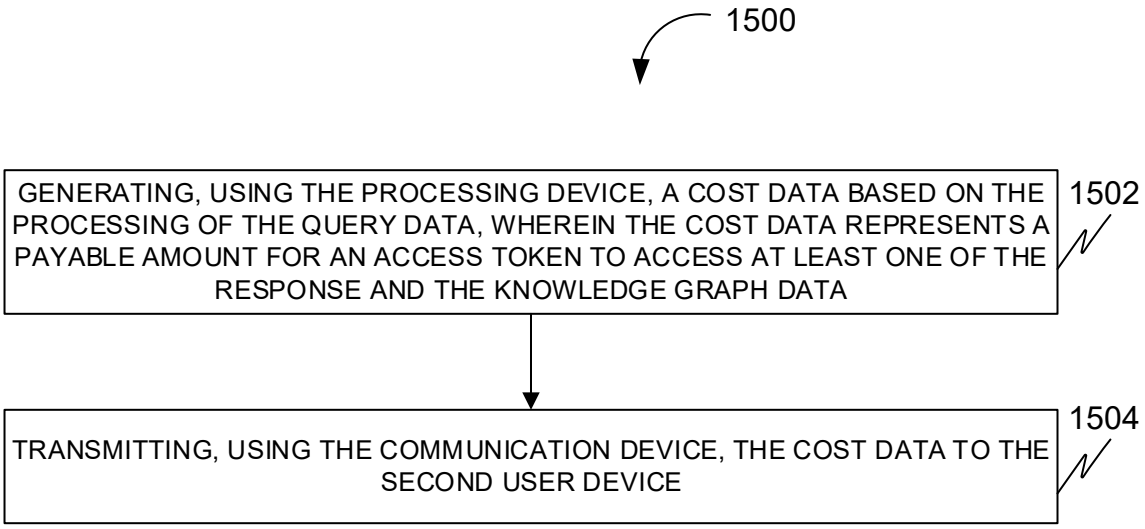

1500
GENERATING, USING THE PROCESSING DEVICE, A COST DATA BASED ON THE PROCESSING OF THE QUERY DATA, WHEREIN THE COST DATA REPRESENTS A PAYABLE AMOUNT FOR AN ACCESS TOKEN TO ACCESS AT LEAST ONE OF THE RESPONSE AND THE KNOWLEDGE GRAPH DATA
1502
TRANSMITTING, USING THE COMMUNICATION DEVICE, THE COST DATA TO THE SECOND USER DEVICE
1504

Fig. 15

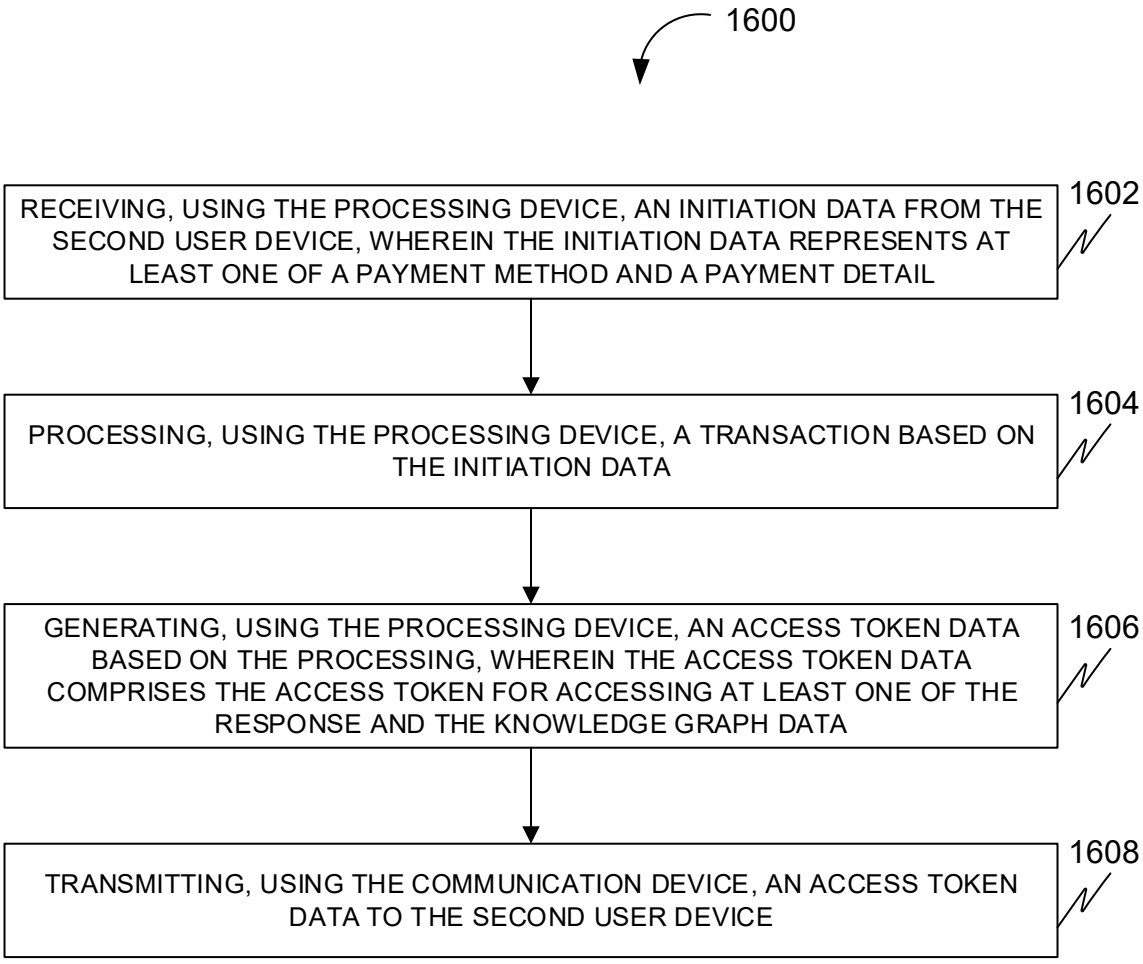

1600
RECEIVING, USING THE PROCESSING DEVICE, AN INITIATION DATA FROM THE SECOND USER DEVICE, WHEREIN THE INITIATION DATA REPRESENTS AT LEAST ONE OF A PAYMENT METHOD AND A PAYMENT DETAIL
1602
PROCESSING, USING THE PROCESSING DEVICE, A TRANSACTION BASED ON THE INITIATION DATA
1604
GENERATING, USING THE PROCESSING DEVICE, AN ACCESS TOKEN DATA BASED ON THE PROCESSING, WHEREIN THE ACCESS TOKEN DATA COMPRISES THE ACCESS TOKEN FOR ACCESSING AT LEAST ONE OF THE RESPONSE AND THE KNOWLEDGE GRAPH DATA
1606
TRANSMITTING, USING THE COMMUNICATION DEVICE, AN ACCESS TOKEN DATA TO THE SECOND USER DEVICE
1608

Fig. 16

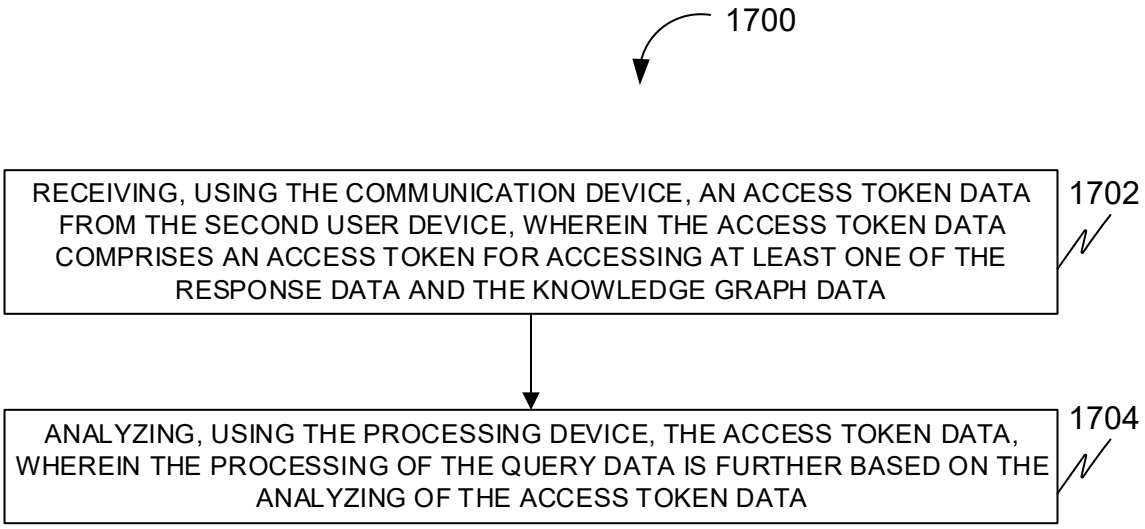

1700
RECEIVING, USING THE COMMUNICATION DEVICE, AN ACCESS TOKEN DATA FROM THE SECOND USER DEVICE, WHEREIN THE ACCESS TOKEN DATA COMPRISES AN ACCESS TOKEN FOR ACCESSING AT LEAST ONE OF THE RESPONSE DATA AND THE KNOWLEDGE GRAPH DATA
1702
ANALYZING, USING THE PROCESSING DEVICE, THE ACCESS TOKEN DATA, WHEREIN THE PROCESSING OF THE QUERY DATA IS FURTHER BASED ON THE ANALYZING OF THE ACCESS TOKEN DATA
1704

Fig. 17

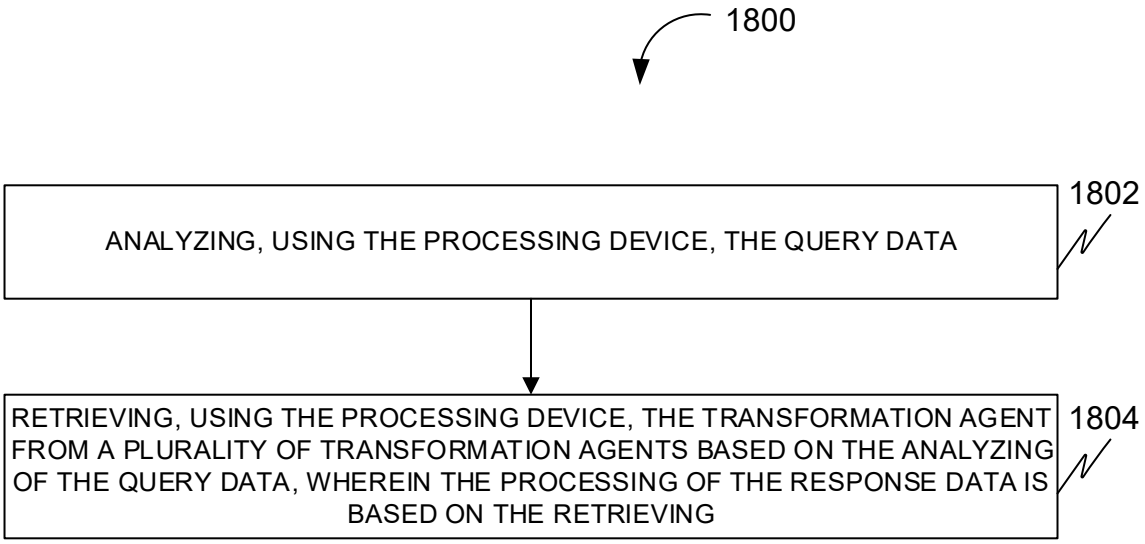

1800
ANALYZING, USING THE PROCESSING DEVICE, THE QUERY DATA
1802
RETRIEVING, USING THE PROCESSING DEVICE, THE TRANSFORMATION AGENT FROM A PLURALITY OF TRANSFORMATION AGENTS BASED ON THE ANALYZING OF THE QUERY DATA, WHEREIN THE PROCESSING OF THE RESPONSE DATA IS BASED ON THE RETRIEVING
1804

Fig. 18

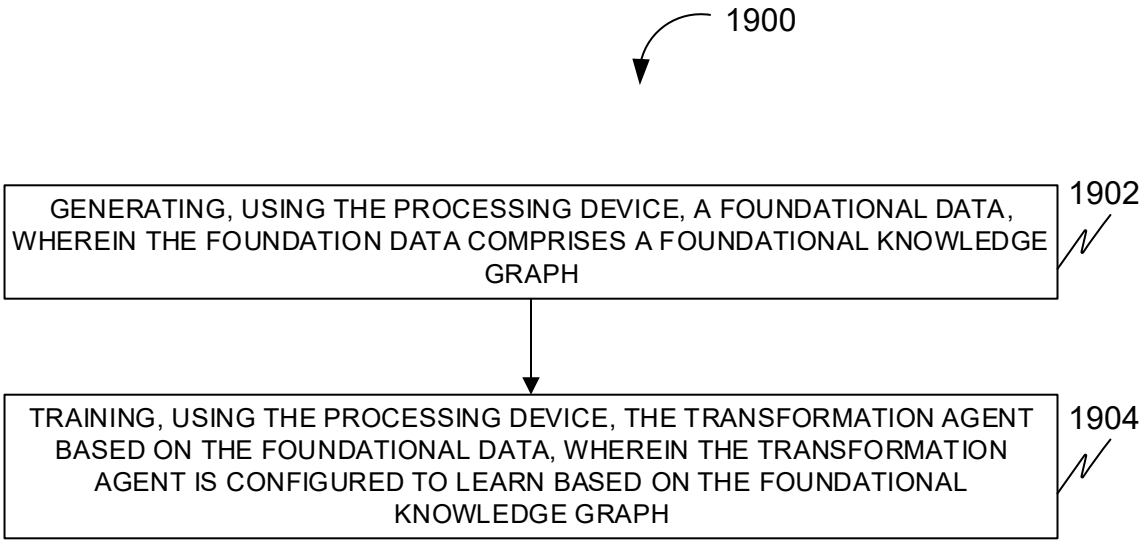

1900
GENERATING, USING THE PROCESSING DEVICE, A FOUNDATIONAL DATA, WHEREIN THE FOUNDATION DATA COMPRISES A FOUNDATIONAL KNOWLEDGE GRAPH
1902
TRAINING, USING THE PROCESSING DEVICE, THE TRANSFORMATION AGENT BASED ON THE FOUNDATIONAL DATA, WHEREIN THE TRANSFORMATION AGENT IS CONFIGURED TO LEARN BASED ON THE FOUNDATIONAL KNOWLEDGE GRAPH
1904

Fig. 19

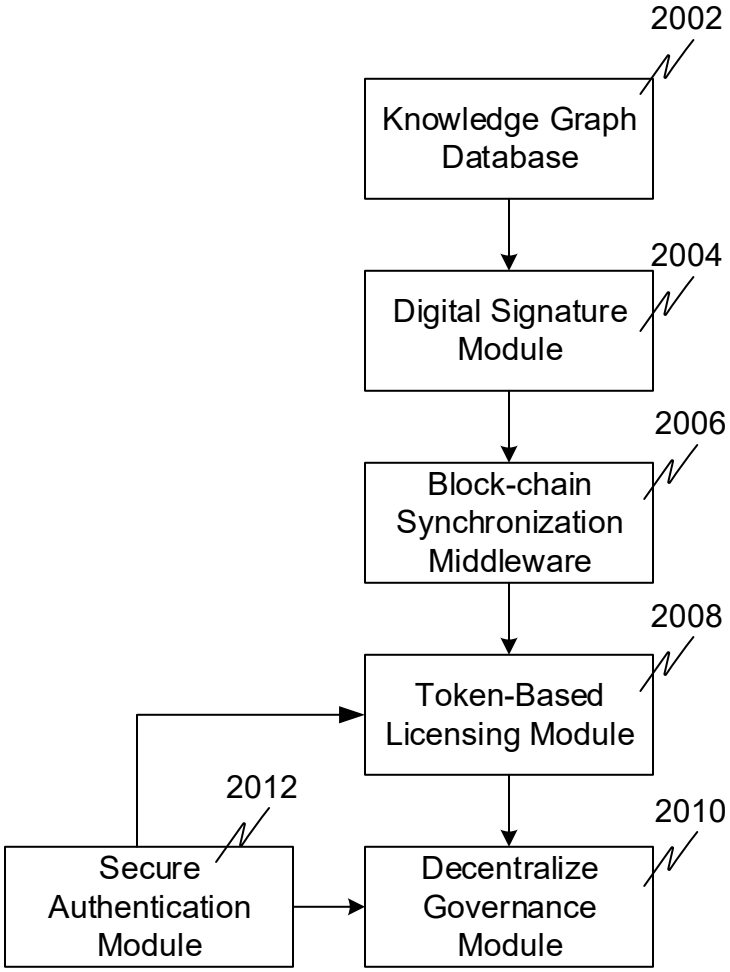

2002
Knowledge Graph Database
2004
Digital Signature Module
2006
Block-chain Synchronization Middleware
2008
Token-Based Licensing Module
2012
Secure Authentication Module
2010
Decentralize Governance Module

Fig. 20

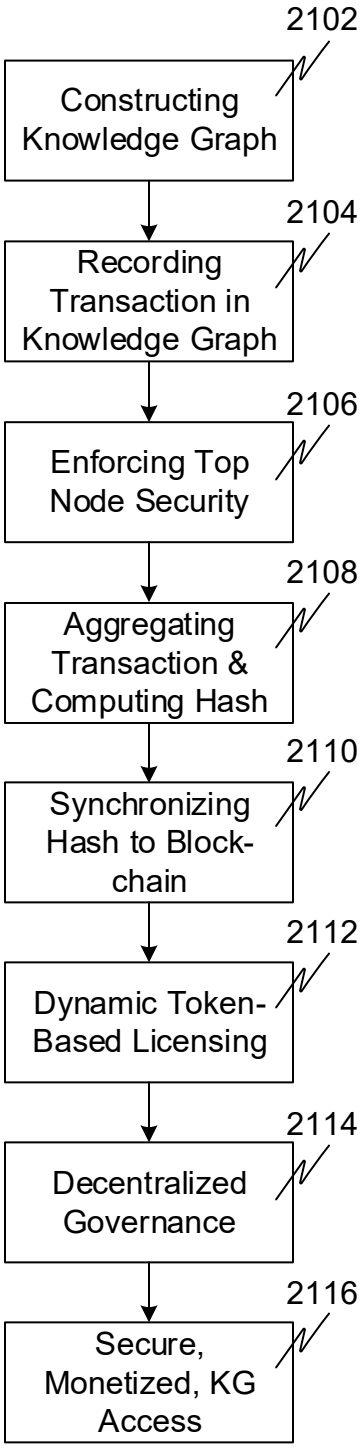

2102
Constructing Knowledge Graph
2104
Recording Transaction in Knowledge Graph
2106
Enforcing Top Node Security
2108
Aggregating Transaction & Computing Hash
2110
Synchronizing Hash to Block-chain
2112
Dynamic Token-Based Licensing
2114
Decentralized Governance
2116
Secure, Monetized, KG Access

Fig. 21

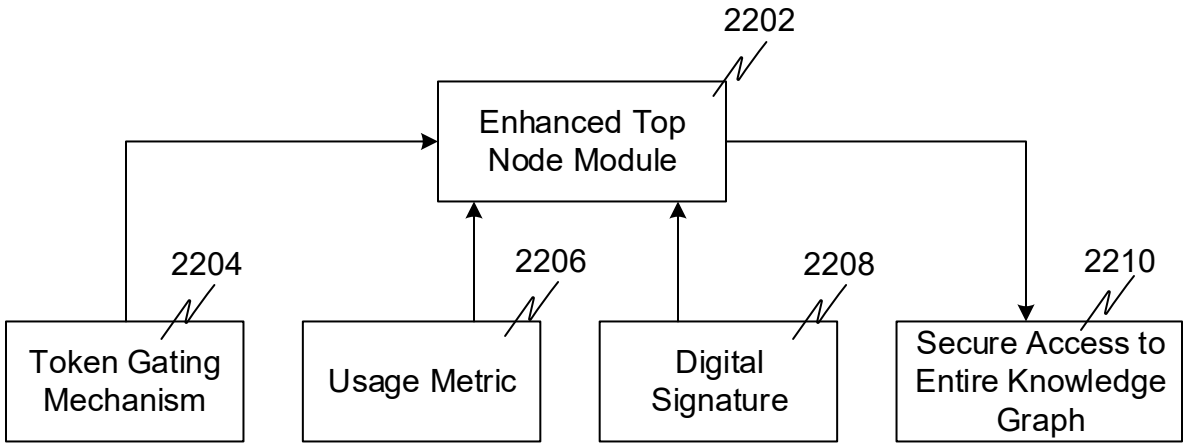

2202
Enhanced Top Node Module
2204
Token Gating Mechanism
2206
Usage Metric
2208
Digital Signature
2210
Secure Access to Entire Knowledge Graph

Fig. 22

Doc Code: MES.GIB
Document Description: Certification of Micro Entity Status (Gross Income Basis)

PTO/SB/15A (07-14)

CERTIFICATION OF MICRO ENTITY STATUS
(GROSS INCOME BASIS)

Application Number or Control Number (if applicable):	Patent Number (if applicable):
First Named Inventor: Richard Gillespie	Title of Invention: METHODS AND SYSTEMS FOR FACILITATING DECENTRALIZED MANAGEMENT OF A KNOWLEDGE GRAPH

The applicant hereby certifies the following—

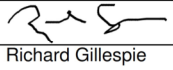
(1) **SMALL ENTITY REQUIREMENT –** The applicant qualifies as a small entity as defined in 37 CFR 1.27.

(2) **APPLICATION FILING LIMIT –** Neither the applicant nor the inventor nor a joint inventor has been named as the inventor or a joint inventor on more than four previously filed U.S. patent applications, excluding provisional applications and international applications under the Patent Cooperation Treaty (PCT) for which the basic national fee under 37 CFR 1.492(a) was not paid, and also excluding patent applications for which the applicant has assigned all ownership rights, or is obligated to assign all ownership rights, as a result of the applicant's previous employment.

(3) **GROSS INCOME LIMIT ON APPLICANTS AND INVENTORS –** Neither the applicant nor the inventor nor a joint inventor, in the calendar year preceding the calendar year in which the applicable fee is being paid, had a gross income, as defined in section 61(a) of the Internal Revenue Code of 1986 (26 U.S.C. 61(a)), exceeding the "Maximum Qualifying Gross Income" reported on the USPTO Web site at http://www.uspto.gov/patents/law/micro_entity.jsp which is equal to three times the median household income for that preceding calendar year, as most recently reported by the Bureau of the Census.

(4) **GROSS INCOME LIMIT ON PARTIES WITH AN "OWNERSHIP INTEREST" –** Neither the applicant nor the inventor nor a joint inventor has assigned, granted, or conveyed, nor is under an obligation by contract or law to assign, grant, or convey, a license or other ownership interest in the application concerned to an entity that, in the calendar year preceding the calendar year in which the applicable fee is being paid, had a gross income, as defined in section 61(a) of the Internal Revenue Code of 1986, exceeding the "Maximum Qualifying Gross Income" reported on the USPTO Web site at http://www.uspto.gov/patents/law/micro_entity.jsp which is equal to three times the median household income for that preceding calendar year, as most recently reported by the Bureau of the Census.

SIGNATURE by an authorized party set forth in 37 CFR 1.33(b)

Signature					
Name	Richard Gillespie				
Date	03/27/2025	Telephone		Registration No.	

☐ There is more than one inventor and I am one of the inventors who are jointly identified as the applicant. The required additional certification form(s) signed by the other joint inventor(s) are included with this form.

Doc Code: PA..
Document Description: Power of Attorney

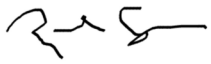
PTO/AIA/82A (07-13)
Approved for use through 03/31/2021. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

NOTE: This form is to be submitted with the Power of Attorney by Applicant form (PTO/AIA/82B) to identify the application to which the Power of Attorney is directed, in accordance with 37 CFR 1.5, unless the application number and filing date are identified in the Power of Attorney by Applicant form. If neither form PTO/AIA/82A nor form PTO/AIA82B identifies the application to which the Power of Attorney is directed, the Power of Attorney will not be recognized in the application.

Application Number	
Filing Date	
First Named Inventor	Richard Gillespie
Title	METHODS AND SYSTEMS FOR FACILITATING DECENTRALIZED MANAGEMENT OF A KNOWLEDGE GRAPH
Art Unit	
Examiner Name	
Attorney Docket Number	TUP89275

SIGNATURE of Applicant or Patent Practitioner

Signature		Date (Optional)	03/27/2025
Name	Richard Gillespie	Registration Number	
Title (if Applicant is a juristic entity)			
Applicant Name (if Applicant is a juristic entity)			

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. If more than one applicant, use multiple forms.

☐ *Total of _____ forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82B (07-13)
Approved for use through 03/31/2021. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

POWER OF ATTORNEY BY APPLICANT

I hereby revoke all previous powers of attorney given in the application identified in either the attached transmittal letter or the boxes below.

Application Number	Filing Date

(Note: The boxes above may be left blank if information is provided on form PTO/AIA/82A.)

☑ I hereby appoint the Patent Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above: 062439

OR

☐ I hereby appoint Practitioner(s) named in the attached list (form PTO/AIA/82C) as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the patent application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above. (Note: Complete form PTO/AIA/82C.)

Please recognize or change the correspondence address for the application identified in the attached transmittal letter or the boxes above to:

☑ The address associated with the above-mentioned Customer Number

OR

☐ The address associated with Customer Number:

OR

☐ Firm or Individual Name					
Address					
City		State		Zip	
Country					
Telephone		Email			

I am the Applicant (if the Applicant is a juristic entity, list the Applicant name in the box):

☑ Inventor or Joint Inventor (title not required below)

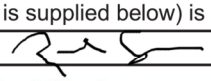
☐ Legal Representative of a Deceased or Legally Incapacitated Inventor (title not required below)

☐ Assignee or Person to Whom the Inventor is Under an Obligation to Assign (provide signer's title if applicant is a juristic entity)

☐ Person Who Otherwise Shows Sufficient Proprietary Interest (e.g., a petition under 37 CFR 1.46(b)(2) was granted in the application or is concurrently being filed with this document) (provide signer's title if applicant is a juristic entity)

SIGNATURE of Applicant for Patent

The undersigned (whose title is supplied below) is authorized to act on behalf of the applicant (e.g., where the applicant is a juristic entity).

Signature		Date (Optional)	03/27/2025
Name	Richard Gillespie		
Title			

NOTE: Signature - This form must be signed by the applicant in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. If more than one applicant, use multiple forms.

☐ Total of forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Doc Code: Oath

Document Description: Oath or declaration filed

PTO/AIA/08 (11-15)
Approved for use through 4/30/2017. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

DECLARATION FOR UTILITY OR DESIGN PATENT APPLICATION (37 CFR 1.63)

☒ Declaration Submitted With Initial Filing OR ☐ Declaration Submitted After Initial Filing (surcharge (37 CFR 1.16(f)) required)

Attorney Docket Number	TUP89275
First Named Inventor	Richard Gillespie
COMPLETE IF KNOWN	
Application Number	
Filing Date	
Art Unit	
Examiner Name	

METHODS AND SYSTEMS FOR FACILITATING DECENTRALIZED MANAGEMENT OF A KNOWLEDGE GRAPH

(Title of the Invention)

As a below named inventor, I hereby declare that:

This declaration is directed to:

☒ The attached application,

OR

☐ United States Application Number or PCT International application number _____

filed on_____.

The above-identified application was made or authorized to be made by me.

I believe I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

Direct all correspondence to: ☒ The address associated with Customer Number: 062439 **OR** ☐ Correspondence address below

Name		
Address		
City	State	Zip
Country	Telephone	Email

PTO/AIA/08 (11-15)
Approved for use through 4/30/2017. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

DECLARATION — Utility or Design Patent Application

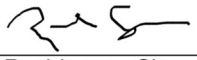
WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available. Petitioner/applicant is advised that documents which form the record of a patent application (such as the PTO/SB/01) are placed into the Privacy Act system of records DEPARTMENT OF COMMERCE, COMMERCE-PAT-7, System name: *Patent Application Files* . Documents not retained in an application file (such as the PTO-2038) are placed into the Privacy Act system of COMMERCE/PAT-TM-10, System name: *Deposit Accounts and Electronic Funds Transfer Profiles*.

LEGAL NAME OF SOLE OR FIRST INVENTOR:

(*E.g.,* Given Name (first and middle if any) and Family Name or Surname)

Richard Gillespie

Inventor's Signature	Date (Optional)
	03/27/2025

Residence: City	State	Country
Norwich	CT	United States

Mailing Address

11 Harbor View Ln

City	State	Zip	Country
Norwich	CT	06360	United States

☐ Additional inventors are being named on the _____ Supplemental sheet(s) PTO/AIA/10 attached hereto

PTO/AIA/14 (01-22)
Approved for use through 05/31/2024. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	TUP89275
	Application Number	
Title of Invention	METHODS AND SYSTEMS FOR FACILITATING DECENTRALIZED MANAGEMENT OF A KNOWLEDGE GRAPH	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2:

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor 1 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Richard		Gillespie	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Norwich	State/Province	CT	Country of Residence	US

Mailing Address of Inventor:

Address 1	11 Harbor View Ln
Address 2	

City	Norwich	State/Province	CT
Postal Code	06360	**Country**	US

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

☐ **An Address is being provided for the correspondence Information of this application.**

Customer Number	62439		
Email Address	patent@sinorica.com	Add Email	Remove Email

Application Information:

Title of the Invention	METHODS AND SYSTEMS FOR FACILITATING DECENTRALIZED MANAGEMENT OF A KNOWLEDGE GRAPH		
Attorney Docket Number	TUP89275	**Small Entity Status Claimed**	☒
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)		**Suggested Figure for Publication (if any)**	

PTO/AIA/14 (01-22)
Approved for use through 05/31/2024. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	TUP89275
	Application Number	
Title of Invention	METHODS AND SYSTEMS FOR FACILITATING DECENTRALIZED MANAGEMENT OF A KNOWLEDGE GRAPH	

Filing By Reference:

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Please Select One:	◉ Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	62439		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, 365(c), or 386(c) or indicate National Stage entry from a PCT application. Providing benefit claim information in the Application Data Sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.
When referring to the current application, please leave the "Application Number" field blank.

Prior Application Status			Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button.

PTO/AIA/14 (01-22)
Approved for use through 05/31/2024. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	TUP89275
	Application Number	
Title of Invention	METHODS AND SYSTEMS FOR FACILITATING DECENTRALIZED MANAGEMENT OF A KNOWLEDGE GRAPH	

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55. When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX)[i] the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(i)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

Remove

Application Number	Country[i]	Filing Date (YYYY-MM-DD)	Access Code[i] (if applicable)

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button.

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

PTO/AIA/14 (01-22)
Approved for use through 05/31/2024. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	TUP89275
	Application Number	
Title of Invention	METHODS AND SYSTEMS FOR FACILITATING DECENTRALIZED MANAGEMENT OF A KNOWLEDGE GRAPH	

Authorization or Opt-Out of Authorization to Permit Access:

When this Application Data Sheet is properly signed and filed with the application, applicant has provided written authority to permit a participating foreign intellectual property (IP) office access to the instant application-as-filed (see paragraph A in subsection 1 below) and the European Patent Office (EPO) access to any search results from the instant application (see paragraph B in subsection 1 below).

Should applicant choose not to provide an authorization identified in subsection 1 below, applicant **must opt-out** of the authorization by checking the corresponding box A or B or both in subsection 2 below.

NOTE: This section of the Application Data Sheet is **ONLY** reviewed and processed with the **INITIAL** filing of an application. After the initial filing of an application, an Application Data Sheet cannot be used to provide or rescind authorization for access by a foreign IP office(s). Instead, Form PTO/SB/39 or PTO/SB/69 must be used as appropriate.

1. Authorization to Permit Access by a Foreign Intellectual Property Office(s)

A. Priority Document Exchange (PDX) - Unless box A in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the State Intellectual Property Office of the People's Republic of China (SIPO), the World Intellectual Property Organization (WIPO), and any other foreign intellectual property office participating with the USPTO in a bilateral or multilateral priority document exchange agreement in which a foreign application claiming priority to the instant patent application is filed, access to: (1) the instant patent application-as-filed and its related bibliographic data, (2) any foreign or domestic application to which priority or benefit is claimed by the instant application and its related bibliographic data, and (3) the date of filing of this Authorization. See 37 CFR 1.14(h)(1).

B. Search Results from U.S. Application to EPO - Unless box B in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the EPO access to the bibliographic data and search results from the instant patent application when a European patent application claiming priority to the instant patent application is filed. See 37 CFR 1.14(h)(2).

The applicant is reminded that the EPO's Rule 141(1) EPC (European Patent Convention) requires applicants to submit a copy of search results from the instant application without delay in a European patent application that claims priority to the instant application.

2. Opt-Out of Authorizations to Permit Access by a Foreign Intellectual Property Office(s)

☐ A. Applicant **DOES NOT** authorize the USPTO to permit a participating foreign IP office access to the instant application-as-filed. If this box is checked, the USPTO will not be providing a participating foreign IP office with any documents and information identified in subsection 1A above.

☐ B. Applicant **DOES NOT** authorize the USPTO to transmit to the EPO any search results from the instant patent application. If this box is checked, the USPTO will not be providing the EPO with search results from the instant application.

NOTE: Once the application has published or is otherwise publicly available, the USPTO may provide access to the application in accordance with 37 CFR 1.14.

PTO/AIA/14 (01-22)
Approved for use through 05/31/2024. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	TUP89275
	Application Number	
Title of Invention	METHODS AND SYSTEMS FOR FACILITATING DECENTRALIZED MANAGEMENT OF A KNOWLEDGE GRAPH	

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Applicant 1

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

◯ Assignee ◯ Legal Representative under 35 U.S.C. 117 ◯ Joint Inventor

◯ Person to whom the inventor is obligated to assign. ◯ Person who shows sufficient proprietary interest

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor:

If the Applicant is an Organization check here. ☐

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Mailing Address Information For Applicant:

Address 1			
Address 2			
City		**State/Province**	
Country		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Applicant Data may be generated within this form by selecting the Add button.

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

PTO/AIA/14 (01-22)
Approved for use through 05/31/2024. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	TUP89275
	Application Number	
Title of Invention	METHODS AND SYSTEMS FOR FACILITATING DECENTRALIZED MANAGEMENT OF A KNOWLEDGE GRAPH	

Assignee 1

Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication. An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.

If the Assignee or Non-Applicant Assignee is an Organization check here. ☐

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1			
Address 2			
City		**State/Province**	
Country i		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button.

Signature:

NOTE: This Application Data Sheet must be signed in accordance with 37 CFR 1.33(b). **However, if this Application Data Sheet is submitted with the INITIAL filing of the application and either box A or B is not checked in subsection 2 of the "Authorization or Opt-Out of Authorization to Permit Access" section, then this form must also be signed in accordance with 37 CFR 1.14(c).**

This Application Data Sheet **must** be signed by a patent practitioner if one or more of the applicants is a **juristic entity** (e.g., corporation or association). If the applicant is two or more joint inventors, this form must be signed by a patent practitioner, **all** joint inventors who are the applicant, or one or more joint inventor-applicants who have been given power of attorney (e.g., see USPTO Form PTO/AIA/81) on behalf of **all** joint inventor-applicants.

See 37 CFR 1.4(d) for the manner of making signatures and certifications.

Signature	/Colby Macias/			Date (YYYY-MM-DD)	2025-03-27
First Name	Colby	Last Name	Macias	Registration Number	76516

Additional Signature may be generated within this form by selecting the Add button.

PTO/AIA/14 (01-22)
Approved for use through 05/31/2024. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	TUP89275
	Application Number	
Title of Invention	METHODS AND SYSTEMS FOR FACILITATING DECENTRALIZED MANAGEMENT OF A KNOWLEDGE GRAPH	

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

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

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

1 The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3 A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent CooperationTreaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.