TRANSACTION AUTHENTICITY VERIFICATION METHOD AND SYSTEM, AND STORAGE MEDIUM

TECHNICAL FIELD

[0001] This specification relates to the field of Internet technologies, and in particular, to a transaction authenticity verification method and system, and a storage medium.

BACKGROUND

[0002] In some transaction scenarios such as cross-border remittance, a large transfer, and a high-risk product transaction, a service platform needs to verify transaction authenticity, to prevent a risk transaction.

[0003] Usually, the transaction authenticity can be verified through manual review. For example, when detecting that a transaction participant initiates a transaction, a service platform can require the transaction participant to upload a certificate material that can prove the transaction authenticity, for example, a certificate material that can prove a fund source, a relationship between transaction participants, logistics information of a transaction product, etc. A review person analyzes the transaction authenticity and transaction rationality based on the certificate material, to ensure transaction security. However, a certificate material of each transaction includes a large amount of information, and the review person needs to take a long period of time to carefully examine and analyze the information, so that review efficiency is low. In addition, a review result is easily affected by a professional level and manual experience of the review person. Consequently, accuracy of a transaction authenticity verification result cannot be ensured. In addition, the service platform needs to train the review person, and person training costs are high.

[0004] Content of the background part is merely information learned of by the inventor, and neither means that the information has entered a public domain before an application date of this disclosure, nor means that the information can become a conventional technology of this disclosure.

SUMMARY

[0005] This specification provides a transaction authenticity verification method and system, and a storage medium, to improve transaction authenticity verification efficiency and reduce a user waiting time. In addition, transaction authenticity verification accuracy and reliability can be improved.

[0006] According to a first aspect, this specification provides a transaction authenticity verification method, including: obtaining transaction information of a target transaction; obtaining a transaction certificate document corresponding to the target transaction, and extracting document key information from the transaction certificate document; obtaining a knowledge graph pre-constructed based on fact data, where the knowledge graph represents a plurality of entities and an association relationship between the plurality of entities, and the plurality of entities include at least an entity corresponding to a transaction participant of the target transaction; and verifying authenticity of the target transaction based on the transaction information, the document key information, and the knowledge graph by using a large model, to obtain an authenticity verification result.

[0007] According to a second aspect, this specification further provides a transaction authenticity verification system, including at least one storage medium and at least one processor. The at least one storage medium stores at least one instruction set, to perform transaction authenticity verification. The at least one processor is communicatively connected to the at least one storage medium, and when the transaction authenticity verification system runs, the at least one processor reads the at least one instruction set, and performs the following operations based on an indication of the at least one instruction set: obtaining transaction information of a target transaction; obtaining a transaction certificate document corresponding to the target transaction, and extracting document key information from the transaction certificate document; obtaining a knowledge graph pre-constructed based on fact data, where the knowledge graph represents a plurality of entities and an association relationship between the plurality of entities, and the plurality of entities include at least an entity corresponding to a transaction participant of the target transaction; and verifying authenticity of the target transaction based on the transaction information, the document key information, and the knowledge graph by using a large model, to obtain an authenticity verification result.

[0008] According to a third aspect, this specification further provides a computer-readable non-transitory storage medium. The computer-readable non-transitory storage medium stores at least one instruction set, and when the at least one instruction set is executed by at least one processor, the method according to any implementation of the first aspect is implemented.

[0009] It can be learned from the above-mentioned technical solutions that, in the transaction authenticity verification method and system, and the storage medium provided in this specification, a computing device can verify authenticity of a target transaction based on transaction information of the target transaction, document key information in a transaction certificate document corresponding to the target transaction, and a pre-constructed knowledge graph by using a large model, to obtain an authenticity verification result. The above-mentioned solution implements automatic authenticity verification on the target transaction by using the large model, to improve verification efficiency, so that a service system can quickly release a transaction and reduce a user waiting time. Because no review person needs to perform manual review, training costs of the review person can be further reduced. Further, in the technical solutions, the large model and the knowledge graph are combined. The knowledge graph can improve a semantic understanding capability of the large model. In addition, the knowledge graph provides the large model with fact information related to a transaction participant of the target transaction, so that the large model can better understand a relationship with the transaction participant of the target transaction. Roles of the knowledge graph in the two aspects can improve accuracy and reliability of performing authenticity verification on the target transaction by the large model.

[0010] Other functions of the transaction authenticity verification method and system, and the storage medium provided in this specification are partially listed in the following descriptions. Creative aspects of the transaction authenticity verification method and system, and the storage medium provided in this specification can be fully explained by practice or by using the methods, apparatuses, and combinations described in the following detailed examples.

BRIEF DESCRIPTION OF DRAWINGS

[0011] To describe the technical solutions in the embodiments of this specification more clearly, the following briefly describes the accompanying drawings needed for describing the embodiments. Clearly, the accompanying drawings in the following descriptions show merely

some embodiments of this specification, and a person of ordinary skill in the art can still derive other drawings from these accompanying drawings without creative efforts.

[0012] FIG. 1 is a schematic diagram of a transaction scenario according to an embodiment of this specification;

[0013] FIG. 2 is a schematic diagram of hardware of a computing device according to an embodiment of this specification;

[0014] FIG. 3 is a flowchart of a transaction authenticity verification method according to an embodiment of this specification;

[0015] FIG. 4 is a schematic diagram of a knowledge graph according to an embodiment of this specification; and

[0016] FIG. 5 is a schematic flowchart of transaction authenticity verification according to an embodiment of this specification.

DESCRIPTION OF EMBODIMENTS

[0017] Specific application scenarios and requirements of this specification are provided in the following descriptions, so that a person skilled in the art can manufacture and use content of this specification. For the person skilled in the art, various local modifications to the disclosed embodiments are clear, and the general principles defined herein can be applied to other embodiments and applications without departing from the spirit and scope of this specification. Therefore, this specification is not limited to the shown embodiments, but has a widest scope consistent with that of the claims.

[0018] The terms used herein are only intended to describe a particular example embodiment, but do not impose a limitation. For example, unless otherwise specified in the context, the singular forms "one", "a", and "the" used herein can also include a plural form. When used in this specification, the terms "include", "comprise", and/or "have" indicate/indicates existence of an associated integer, step, operation, element, and/or component, but does not exclude existence of one or more other features, integers, steps, operations, elements, components, and/or groups, or another feature, integer, step, operation, element, component, and/or group can be added to the system/method.

[0019] In consideration of the following descriptions, these and other features of this

specification, operations and functions of related components of the structure, and economy of combination and manufacturing of components can be significantly improved. With reference to the accompanying drawings, all of these form a part of this specification. However, it should be clearly understood that the accompanying drawings are merely used for the purpose of illustration and description, and are not intended to limit the scope of this specification. It should be further understood that the accompanying drawings are not drawn to scale.

[0020] The flowchart used in this specification illustrates operations implemented by a system in some embodiments of this specification. It should be clearly understood that operations in the flowchart can be implemented out of sequence. On the contrary, operations can be implemented reversely or simultaneously. In addition, one or more other operations can be added to the flowchart. One or more operations can be removed from the flowchart.

[0021] Before specific embodiments of this specification are described, an application scenario to which the technical solutions provided in this specification are applicable is first described.

[0022] The technical solutions provided in this specification are applicable to a scenario in which authenticity of a transaction is verified. Authenticity verification of the transaction can also be briefly referred to as transaction authenticity verification. In this specification, authenticity verification of the transaction can be performing a series of methods and procedures to determine that information such as a motivation, content, an amount, and a participant of the transaction is accurate and complies with related provisions of the law, to ensure authenticity and rationality of the transaction.

[0023] For example, in a cross-border remittance transaction scenario, authenticity verification of the transaction is a key process of risk transaction prevention and control. For example, when detecting that a remitter initiates a remittance request or detecting that a remittee initiates a collection request, a service platform can require the remitter or the remittee to upload a transaction certificate document used to prove authenticity of the transaction. Further, the service platform can verify the authenticity of the transaction based on the transaction certificate document, to obtain an authenticity verification result corresponding to the transaction. For example, if the transaction is not a real transaction, it is considered that the transaction has a risk, and the transaction can be intercepted. If the transaction is a real transaction, it is considered that the transaction has no risk, and the transaction can be released.

[0024] It should be noted that the cross-border remittance transaction scenario is only one of a plurality of use scenarios to which embodiments of this specification are applied. A transaction authenticity verification method provided in embodiments of this specification can be applied not only to the cross-border remittance transaction scenario, but also to another transaction scenario, for example, a large transfer or a high-risk product transaction. Examples are not listed one by one herein.

[0025] Usually, after detecting a transaction request initiated by a transaction participant (for example, a remitter or remittee) for a target transaction, the service platform can request the transaction participant to upload a transaction certificate document. It can be understood that, for different transaction types, the service platform can need different transaction certificate documents uploaded by the transaction participant. For example, if the transaction type is trade remittance, the service platform can require the transaction participants to upload the following transaction certificate documents: a transaction contract, an invoice, and a logistics certificate document (for example, a logistics bill or a bill of lading). For example, if the transaction type is relative remittance, the service platform can require the transaction participant to upload the following transaction certificate document: a certificate document (for example, a marriage certificate) used to prove a relationship between transaction participants of the target transaction.

[0026] Before the transaction participant performs a transaction operation, the service platform can remind the transaction participant to upload the transaction certificate document. Alternatively, after the transaction participant performs a transaction operation, the service platform can remind the transaction participant to upload the transaction certificate document. Alternatively, in a process of performing transaction authenticity verification on the target transaction, if a review person finds that some transaction certificate documents are missing, the service platform can notify the transaction participant to hand over the supplementary missing transaction certificate document. This specification sets no limitation on an uploading timing of the transaction certificate document.

[0027] After receiving the transaction certificate document uploaded by the transaction participant, the service platform can store the transaction certificate document, and generate a transaction authenticity verification task corresponding to the target transaction. The service platform can add the transaction authenticity verification task to a task queue. It can be understood that the service platform can maintain an ordered task queue based on a sequence of the transaction

request. The service platform can assign all transaction authenticity verification tasks in the task queue to different review persons. After receiving the transaction authenticity verification task corresponding to the target transaction, the review person can trigger transaction authenticity verification of the target transaction.

[0028] When performing authenticity verification on the target transaction, the review person can obtain transaction information of the target transaction and a transaction certificate document corresponding to the target transaction. The review person analyzes authenticity and rationality of the target transaction based on the transaction certificate document. If the review person considers that the target transaction is not a real transaction, the service platform can intercept the target transaction. If the review person considers that the target transaction is a real transaction, the service platform can release the target transaction.

[0029] Because the transaction certificate document includes a large amount of information, the review person needs to carefully check and analyze the information for a long period of time. Therefore, review efficiency is low. In addition, a manual review manner depends on experience of the review person. A review person with insufficient experience is limited to proficiency of the review person, and a transaction authenticity analysis result is not accurate. Even for a very skilled review person, there is a working error, and therefore, the transaction authenticity analysis result is not accurate. In addition, the service platform needs to train the review person for a long period of time, and person training costs are high.

[0030] Therefore, embodiments of this specification provide a transaction authenticity verification method and system, and a storage medium. When a service platform needs to perform authenticity verification on a target transaction, the service platform can verify, by using a large model, authenticity of the target transaction based on transaction information of the target transaction, document key information in a transaction certificate document corresponding to the target transaction, and a knowledge graph pre-constructed based on fact data, to obtain an authenticity verification result. In the above-mentioned solution, automatic transaction authenticity verification is implemented by using the large model, and a review person does not need to manually review the transaction certificate document. This improves transaction authenticity verification efficiency and reduces training costs of the service platform for the review person. In the above-mentioned solution, the knowledge graph is constructed based on the fact data, and can reflect an association relationship between an entity corresponding to a transaction

participant of the target transaction and another entity. Therefore, the large model performs transaction authenticity verification based on the knowledge graph, to improve accuracy of a transaction authenticity verification result.

[0031] FIG. 1 is a schematic diagram of a transaction scenario 100 according to an embodiment of this specification. The transaction scenario 100 can be any transaction scenario, for example, a cross-border remittance scenario, a large transfer scenario, or a high-risk product transaction scenario.

[0032] As shown in FIG. 1, the transaction scenario 100 can include a user 110, a terminal device 120, a server 130, and a network 140. The user 110 can initiate a transaction on a service platform. The terminal device 120 can serve as a client of the service platform, or the terminal device 120 is deployed with a client of the service platform. The server 130 can serve as a serving end of the service platform, or the server 130 is deployed with a serving end of the service platform. In some embodiments, a transaction authenticity verification scenario 100 can further include a verification device (not shown).

[0033] The user 110 can be a user who triggers a transaction, and the user 110 can execute a related event by using the terminal device 120. For example, the user 110 initiates a transaction request on the terminal device 120. In some cases, the user 110 can further perform, on the terminal device 120, an operation of uploading a transaction certificate document. In some embodiments, the terminal device 120 is installed with one or more apps, and the one or more apps can provide the user 110 with a capability of executing the related event. The app includes but is not limited to a web browser app, a search app, a chat app, a shopping app, a service app, a video app, a financial app, a payment app, etc. Usually, the user 110 can be a transaction participant of the transaction, for example, can be a supply party of the transaction (in this case, the user 110 can also be referred to as a merchant or a seller), or can be a demand party of the transaction (in this case, the user 110 can also be referred to as a buyer or a consumer).

[0034] The terminal device 120 can present an interaction interface to the user, so that the user 110 executes some events in the interaction interface. Specifically, the user 110 can initiate a transaction request in the interaction interface. The user 110 can further upload the transaction certificate document in the interaction interface.

[0035] In some embodiments, the terminal device 120 can include a mobile device, a tablet computer, a laptop computer, a device built in a motor vehicle or similar content, or any

combination thereof. In some embodiments, the mobile device can include a smart home device, a smart mobile device, a virtual reality device, an augmented reality device or a similar device, or any combination thereof. In some embodiments, the smart home apparatus can include a smart television, a desktop computer, or any combination. In some embodiments, the smart mobile device can include a smartphone, a personal digital assistant, a game device, a navigation device, or any combination thereof. In some embodiments, the virtual reality device or the augmented reality device can include a virtual reality helmet, virtual reality glasses, a virtual reality handle, an augmented reality helmet, augmented reality glasses, an augmented reality handle or similar content, or any combination thereof. For example, the virtual reality device or the augmented reality device may include smart glasses, a head mounted display, and VR. In some embodiments, the apparatus built in the motor vehicle can include a vehicle-mounted computer, a vehicle-mounted television, etc.

[0036] In some embodiments, a transaction authenticity verification method described below in this specification can be performed on the terminal device 120. For example, the terminal device 120 can perform the transaction authenticity verification method described in this specification in response to the transaction request triggered by the user 110. In this case, the terminal device 120 can store data or instructions used to implement the transaction authenticity verification method, and can execute or be configured to execute the data or the instructions. In some embodiments, the terminal device 120 can include a hardware device with a data information processing function and a necessary program needed for driving the hardware device to work.

[0037] In some embodiments, one or more application programs (app) can be installed on the terminal device 120. The app can provide the user 110 with a capability and an interface for interacting with the outside through the network 140. The app includes but is not limited to a web browser app program, a search app program, a chat app program, a shopping app program, a video app program, a financial app program, an instant messaging tool, a mailbox terminal device, a social platform software, etc. In some embodiments, a target app can be installed on the terminal device 120. In some embodiments, the user 110 can trigger the transaction request by using the target app, or can upload the transaction certificate document by using the target app. The target app can perform the transaction authenticity verification method described in this specification in response to the transaction request.

[0038] In some embodiments, as shown in FIG. 1, the terminal device 120 can be

communicatively connected to the server 130. The server 130 can be a server that provides various services, for example, a backend server that provides a transaction service for the terminal device 120. In some embodiments, the terminal device 120 can interact with the server 130 through the network 140, to receive or send a message, etc. For example, the terminal device 120 can send a transaction certificate document related to the transaction to the server 130. The server 130 can be communicatively connected to a plurality of terminal devices 120, and separately receive a transaction certificate document sent by each terminal device 120.

[0039] In some embodiments, the transaction authenticity verification method described below in this specification can be performed on the server 130. In this case, the server 130 can store data or instructions used to implement the transaction authenticity verification method, and can execute or be configured to execute the data or the instructions. In some embodiments, the server 130 can include a hardware device with a data information processing function and a necessary program needed for driving the hardware device to work.

[0040] In some embodiments, the transaction authenticity verification scenario 100 can further include a verification device. The verification device is an electronic device with a certain data processing capability. In this case, the verification device can store data or instructions used to implement the transaction authenticity verification method described in this specification, and can execute or be configured to execute the data or the instructions. For example, the verification device can include a hardware device with a data information processing function and a necessary program required for driving the hardware device to work. In some embodiments, the verification device and the server 130 can be deployed on one physical device. In this case, the verification device can serve as a unit/module in the server 300. The verification device and the server 130 can also be deployed on different entity devices. This is not limited herein.

[0041] In some embodiments, the server 130 generates a corresponding transaction authenticity verification task after receiving the transaction certificate document related to the transaction, and adds the transaction authenticity verification task to a task queue. It can be understood that the server 130 can maintain an ordered task queue based on a sequence of the transaction request. The server 130 can distribute a transaction authenticity verification task in the task queue to the verification device, or the verification device requests one or more transaction authenticity verification tasks from the server 130. After obtaining the one or more transaction authenticity verification tasks, the verification device performs authenticity verification on the

transaction. After obtaining a transaction authenticity verification result of the transaction, the verification device can feed back the transaction authenticity verification result to the server 130, so that the server 130 performs subsequent processing on the transaction based on the transaction authenticity verification result. For example, if the server 130 determines, based on the transaction authenticity verification result, that the transaction is a risk transaction, prompt information is sent to the user 110 by using the terminal device 120. For example, the prompt information is "A current transaction has a risk and the transaction is intercepted". If the server 130 determines, based on the transaction authenticity verification result, that the transaction has no risk, prompt information is displayed to the user 110 by using the terminal device 120. For example, the prompt information is "A current transaction has no risk and the transaction is completed."

[0042] The network 140 is a medium for providing a communication connection between the terminal device 120 and the server 130 and between the server 130 and the verification device. The network 140 can facilitate exchange of information or data. In some embodiments, the network 140 can be any type of wired or wireless network, or a combination thereof. For example, the network 140 can include a cable network, a wired network, an optical fiber network, a telecommunications network, an intranet, the Internet, a local area network (LAN), a wide area network (WAN), a wireless local area network (WLAN), a metropolitan area network (MAN), a public switched telephone network (PSTN), a Bluetooth network, a ZigBee network, a near field communication (NFC) network, or a similar network. In some embodiments, the network 140 can include one or more network access points. For example, the network 140 can include a wired or wireless network access point, for example, a base station or an Internet switching point. Through the access point, one or more components in the terminal device 120 and the server 130 can be connected to the network 140 to exchange data or information.

[0043] It should be understood that quantities of terminal devices 120, servers 130, and networks 140 in FIG. 1 are merely examples. Based on an implementation requirement, there can be any quantity of terminal devices 120, servers 130, networks 140, and verification devices.

[0044] FIG. 2 is a schematic diagram of hardware of a computing device 200 according to an embodiment of this specification. The computing device 200 can perform a transaction authenticity verification method provided in this specification. In some embodiments, the computing device 200 can serve as the server 130 in FIG. 1, to perform the transaction authenticity verification method. In some embodiments, the computing device 200 can serve as the terminal device 120 in

FIG. 1, to perform the transaction authenticity verification method. In some embodiments, the computing device 200 can serve as the verification device in FIG. 1, to perform the transaction authenticity verification method. The computing device 200 can further correspond to a transaction authenticity verification system provided in this specification.

[0045] As shown in FIG. 2, the computing device 200 can include at least one storage medium 230 and at least one processor 220. In some embodiments, the computing device 200 can further include a communication port 250 and an internal communication bus 210. The computing device 200 can further include an I/O component 240.

[0046] The internal communication bus 210 can be connected to different system components, including a storage medium 230, a processor 220, and a communication port 250.

[0047] The I/O component 240 supports input/output between the computing device 200 and other components.

[0048] The communication port 250 is used for data communication between the computing device 200 and the outside. For example, the communication port 250 can be used for data communication between the computing device 200 and a network 140. The communication port 250 can be a wired communication port, or can be a wireless communication port.

[0049] The storage medium 230 can include a data storage apparatus. The data storage apparatus can be a non-transitory storage medium, or can be a transitory storage medium. For example, the data storage apparatus can include one or more of a disk 232, a read-only storage medium (ROM) 234, or a random access storage medium (RAM) 236. The storage medium 230 further includes at least one instruction set stored in the data storage apparatus. The instruction set can be computer program code. The computer program code can include a program, a routine, an object, a component, a data structure, a process, a module, etc. for performing the transaction authenticity verification method provided in this specification.

[0050] The processor 220 is communicatively connected to the storage medium 230. The processor 220 is configured to execute the at least one instruction set. When the computing device 200 runs, the processor 220 reads the at least one instruction set, and performs, based on an indication of the at least one instruction set, the transaction authenticity verification method provided in this specification. The processor 220 can perform all steps included in the transaction authenticity verification method. The processor 220 can be in a form of one or more processors. In some embodiments, the processor 220 can include one or more hardware processors, for

example, a microcontroller, a microprocessor, a reduced instruction set computer (RISC), an application-specific integrated circuit (ASIC), an application-specific instruction set processor (ASIP), a central processing unit (CPU), a graphics processing unit (GPU), a physical processing unit (PPU), a microcontroller unit, a digital signal processor (DSP), a field programmable gate array (FPGA), an advanced RISC machine (ARM), a programmable logic device (PLD), any circuit or processor that can perform one or more functions, or any combination thereof.

[0051] For illustration purposes only, FIG. 2 shows only a case in which the computing device 200 includes one processor 220. However, it should be noted that, the computing device 200 in this specification can further include a plurality of processors 220. Therefore, the operations and/or method steps disclosed in this specification can be performed by one processor, or can be jointly performed by a plurality of processors. For example, if the processor 220 in the computing device 200 in this specification performs step A and step B, it should be understood as that step A and step B can be jointly or separately performed by two different processors 220 (for example, a first processor performs step A, and a second processor performs step B, or a first processor and a second processor jointly perform steps A and B).

[0052] FIG. 3 is a flowchart of a transaction authenticity verification method P300 according to an embodiment of this specification. As described above, the computing device 200 shown in FIG. 2 can perform the transaction authenticity verification method P300. Specifically, a processor 220 in the computing device 200 can read an instruction set stored in a local storage medium of the computing device 200, and then perform the transaction authenticity verification method P300 based on a stipulation of the instruction set.

[0053] As shown in FIG. 3, the transaction authenticity verification method P300 can include the following steps.

[0054] S310: Obtain transaction information of a target transaction.

[0055] The target transaction is a transaction on which authenticity verification is to be performed. The transaction information of the target transaction is related information used to describe the target transaction. The transaction information of the target transaction can include but is not limited to related information of a transaction participant, a transaction amount, a subject matter of the transaction, etc.

[0056] S320: Obtain a transaction certificate document corresponding to the target transaction, and extract document key information from the transaction certificate document.

[0057] The transaction certificate document can be a document uploaded by the transaction participant of the target transaction to prove authenticity of the target transaction. For example, when a service platform detects that the transaction participant initiates the target transaction, the service platform can provide a document upload entry to the transaction participant, and the transaction participant can upload the transaction certificate document through the document upload entry. The transaction certificate document includes but is not limited to: a document used to prove an identity, a document used to prove a fund transaction, a document used to prove a trade transaction, etc. The document used to prove an identity can include an identity card, a passport, a marriage certificate, a birth certificate, etc. The document used to prove a fund transaction can include a salary sheet, an employment certificate, a labor contract, a tax bill, etc. The document used to prove a trade transaction can include a shopping website screenshot, a logistics bill, a service agreement, etc.

[0058] The document key information can be information that is included in the transaction certificate document and that needs to be paid attention to in a transaction authenticity verification process. In different transaction scenarios or for different types of transaction certificate documents, document key information that need to be extracted can be different. Content of the document key information is not limited in this specification. For example, when the transaction certificate document is a logistics bill, document key information that needs to be extracted can include a bill number, a participant, a transaction date, transaction content, a subject matter of a transaction, etc. When the transaction certificate document is a salary sheet, the document key information that needs to be extracted can include a salary amount, a tax amount, a transaction time, transaction account information, etc.

[0059] This specification sets no limitation on types and a quantity of transaction certificate documents. A person skilled in the art can understand that types and quantities of transaction certificate documents that need to be uploaded in different transaction scenarios can be different. For example, in a relative transaction scenario, the transaction certificate document that needs to be uploaded by the transaction participant can include the document used to prove an identity and the document used to prove a fund transaction. For another example, in a trade transaction scenario, the transaction certificate document that needs to be uploaded by the transaction participant can include the document used to prove a trade transaction.

[0060] After obtaining the transaction certificate document corresponding to the target

transaction, the computing device 200 can perform text recognition on the transaction certificate document, to obtain a text recognition result. The transaction certificate document can be in various formats such as a picture format and a text format. If the transaction certificate document is in a picture format, the computing device 200 can perform text recognition on the transaction certificate document by using an optical character recognition (OCR) technology, to obtain a text recognition result. If the transaction certificate document is in a text format, the computing device 200 can perform text recognition on the transaction certificate document by using a named entity recognition (NER) technology, to obtain a text recognition result. If the transaction certificate document is in another format, the computing device 200 can obtain a text recognition result by using a text recognition technology corresponding to another format.

[0061] In a cross-border transaction scenario, transaction certificate documents corresponding to different transactions may have different languages. In a text recognition process, for example, the computing device 200 can first translate transaction certificate documents in different languages into a target language. The target language can be, for example, Chinese, or certainly can be English, Japanese, or another target language. Subsequently, the computing device 200 performs text recognition based on the translated transaction certificate document.

[0062] The computing device 200 can further determine a document type corresponding to the transaction certificate document. The document type can include but is not limited to an identity voucher, a marriage certificate, a fund transaction certificate, a salary sheet, an employment certificate, a labor contract, a tax bill, a shopping website screenshot, a logistics bill, a service agreement, etc. It should be understood that the listed document types are merely example descriptions. This specification sets no limitation thereto.

[0063] The computing device 200 can determine the document type in a plurality of manners. The following provides descriptions by using three manners as examples.

[0064] Manner 1: The computing device 200 can determine the document type based on the text recognition result. Specifically, after obtaining the text recognition result, the computing device 200 determines the document type by performing keyword or key sentence analysis on the text recognition result.

[0065] For example, if the text recognition result includes "It is hereby proved that Mr. Tom is employed by our company for more than three years", the computing device 200 determines, by analyzing the text recognition result, that the document type is the employment certificate.

[0066] Manner 2: The computing device 200 can determine the document type based on layout information of the transaction certificate document. Different types of transaction certificate documents have different layout features such as an identifier, a watermark, and a table structure. For example, a bank bill usually includes a bank logo, account information, and a transaction record list that are arranged in a specific layout manner. For another example, the marriage certificate usually includes a civil affairs bureau seal, a marriage date, etc. that are arranged in a specific layout manner. The computing device 200 can compare the layout information of the transaction certificate document with standard layout information of different types of documents, to determine the document type corresponding to the transaction certificate document.

[0067] Manner 3: The computing device 200 can determine the document type based on a name of the transaction certificate document. When the transaction participant uploads the transaction certificate document, the transaction certificate document is usually provided with a file name. The computing device 200 can determine the document type based on the file name.

[0068] For example, if a file name of a specific transaction certificate document is "Tom_employment certificate.pdf", the computing device 200 can determine, based on the file name, that the type of the transaction certificate document is an employment certificate.

[0069] There can be one or more transaction certificate documents. When there are a plurality of transaction certificate documents, the computing device 200 can separately perform text recognition on the transaction certificate documents, and separately determine document types.

[0070] After determining the document type corresponding to the transaction certificate document, the computing device 200 can perform information extraction on the text recognition result based on the document type corresponding to the transaction certificate document, to obtain the document key information corresponding to a target transaction document.

[0071] In the above-mentioned embodiments, the computing device 200 performs information extraction on the text recognition result based on the document type, to obtain the document key information. In this way, accuracy of the document key information can be ensured. In addition, an implementation is simple, and time costs required for obtaining the document key information can be reduced.

[0072] In some embodiments, the computing device 200 can perform information extraction on the text recognition result based on an information extraction model, to obtain the document key information. For example, the computing device 200 can be deployed with a plurality of

information extraction models. Different information extraction models correspond to different document types, and are applicable to information extraction on documents of different document types. Each information extraction model can be obtained through training based on a large quantity of sample documents (a sample document of a document type corresponding to the information extraction model). One information extraction model can correspond to one document type, or can correspond to a plurality of document types. This is not limited in this specification.

[0073] For example, the plurality of information extraction models can include an identity information extraction model, a fund transaction certificate type information extraction model, and a trade document information extraction model. The identity information extraction model is used to perform information extraction on the transaction certificate document such as an identity certificate, a passport, and a marriage certificate. The identity information extraction model focuses on identity information (for example, a certificate code, a certificate validity period information) and relationship information (for example, a relationship between two parties) in the transaction certificate document. The fund transaction certificate information extraction model is used to perform information extraction on a transaction certificate document of a fund transaction certificate type. The fund transaction certification information extraction model focuses on fund transaction related information in the transaction certificate document, for example, a salary, a tax, a transaction amount, a transaction time, and transaction account information. The trade document information extraction model is used to perform information extraction on the transaction certificate document such as a logistics bill, a contract, or a protocol. The trade document information extraction model focuses on trade related information in the transaction certificate document, for example, a trade document number, a trade participant, a transaction date, transaction content, and a subject matter of a transaction.

[0074] When performing information extraction, the computing device 200 can determine a target information extraction model corresponding to the document type from the plurality of information extraction models, and further, perform information extraction on the text recognition result by using the target information extraction model, to obtain the document key information in the transaction certificate document.

[0075] For example, if the transaction certificate document is a marriage certificate, the computing device 200 can perform information extraction on the text recognition result of the transaction certificate document by using the identity information extraction model, to obtain the

document key information. If the transaction certificate document is a logistics bill, the computing device 200 can perform information extraction on the text recognition result of the transaction certificate document by using the trade document information extraction model, to obtain the document key information.

[0076] In the above-mentioned embodiments, for different types of transaction certificate documents, the document key information can be extracted by using different information extraction models, so that information extraction for the transaction certificate document is more specific. In this way, accuracy of the extracted document key information is improved. In addition, the computing device 200 can perform information extraction on the transaction certificate document in a complex scenario.

[0077] S330: Obtain a knowledge graph pre-constructed based on fact data, where the knowledge graph represents a plurality of entities and an association relationship between the plurality of entities, and the plurality of entities include at least an entity corresponding to a transaction participant of the target transaction.

[0078] The knowledge graph is a structured knowledge representation method, describes an entity (for example, a person, a location, or a concept) and an association relationship between different entities in a form of a graph, and is intended to store and present knowledge in the world in a machine readable form. The knowledge graph constructed based on the fact data can be understood as follows: The knowledge graph is constructed based on objective information that exists in a real world.

[0079] In some embodiments, the knowledge graph can be a private knowledge graph, namely, a knowledge graph constructed based on historical data accumulated on the service platform. In some embodiments, the knowledge graph can alternatively be a common knowledge graph, namely, a knowledge graph constructed based on open knowledge of an external platform.

[0080] In this specification, the knowledge graph can represent/describe/reflect a plurality of entities and an association relationship between the plurality of entities. The knowledge graph can include the following elements: an entity, an attribute, and a relationship. The entity is a basic constitutional unit in the knowledge graph, and represents an object in the real world. For example, the entity can be a city (for example, a city A), can be a person (for example, Tom), or can be a concept (for example, relativity). The attribute is used to describe a feature or a status of an entity, and can be considered as affiliated information of the entity. For example, an attribute of the entity

"Tom" can include "occupation", "place of residence", etc. For another example, an attribute of the entity "city A" can include "area", "population", etc. The relationship represents the relationship between different entities, and is a key of expressing knowledge in the knowledge graph. For example, a relationship between "Einstein" and "relativity" can be "proposed", and a relationship between "Tom" and "Jim" can be "couple".

[0081] The knowledge graph can be presented in a form of a node and an edge. The node corresponds to an entity and an attribute. An edge between different nodes represents a relationship between two nodes. For example, an edge between an entity and an attribute of the entity represents an affiliated relationship between the entity and the attribute. An edge between different entities represents an association relationship between entities.

[0082] Specifically, FIG. 4 is a schematic diagram of a knowledge graph according to an embodiment of this specification. As shown in FIG. 4, the knowledge graph includes an entity node, for example, Tom, Jim, and David. The knowledge graph further includes an attribute node, for example, a country E, a country F, an engineer, unemployed, a student, etc.

[0083] The edge between different entity nodes represents an association relationship between different entities. For example, an edge between Tom and Jim represents a couple relationship between Tom and Jim, an edge between Jim and David represents a parent-child relationship between Jim and David, and an edge between Tom and David represents a mother-child relationship between Tom and David. An edge between the entity node and the attribute node represents an affiliated relationship between the entity and the attribute. For example, affiliated information of Tom includes "unemployed" and "located in a country E"; affiliated information of Jim includes "located in a country F" and "an occupation is an engineer"; and affiliated information of David includes "located in a country E" and "an entity is a student".

[0084] It can be understood that an edge between nodes in the knowledge graph can be a directed edge, or can be an undirected edge. FIG. 4 shows an example of the directed edge. This is not limited in this embodiment of this specification.

[0085] In some embodiments, the knowledge graph can be pre-stored in a database or pre-stored in storage space of the computing device 200. When performing S330, the computing device 200 can obtain the knowledge graph from the database or obtain the knowledge graph from the storage space of the computing device 200. In this specification, the knowledge graph obtained by the computing device 200 in S330 includes at least an entity corresponding to the transaction

participant of the target transaction. For example, the target transaction is a transaction between Tom and Jim. In other words, the transaction participant of the target transaction includes Tom and Jim, and each entity in the knowledge graph includes at least the entity "Tom" and the entity "Jim".

[0086] The following describes a process of constructing the knowledge graph. It should be noted that the process of constructing the knowledge graph can be performed by the computing device 200, or can be performed by another device. This is not limited in this specification. The computing device 200 is used as an example for description in the following descriptions.

[0087] The computing device 200 can obtain historical data generated in a historical time period, and generate the knowledge graph by analyzing the historical data.

[0088] The historical data can include data generated in the historical time period on a current service platform (for example, a platform that generates the target transaction), and can further include data generated in the historical time period on another service platform (for example, a social service platform or a location service platform). The historical data includes at least one of social data, transaction data, and geographic location data. The social data can include attribute information of each of a plurality of entities, an association relationship between the plurality of entities, etc. The transaction data can include related information of a transaction generated between different entities in the plurality of entities, for example, a transaction amount and a transaction time. The geographic location data includes location information of each of the plurality of entities.

[0089] In some embodiments, when generating service data (for example, transaction data, social data, or geographic location data), the current service platform can store the service data in a target database. When generating the service data, another service platform can store the service data in the target database. Alternatively, the current service platform can synchronize service data from another service platform based on a specific time period, and store synchronized data in the target database. In this way, the target database stores historical data (namely, service data) generated by the current service platform and/or the another service platform. When the computing device 200 needs to construct the knowledge graph, the historical data generated in the historical time period can be obtained from the target database.

[0090] After obtaining the historical data, the computing device 200 can analyze the historical data, to obtain an entity involved in the historical data and an association relationship between different entities; and generate the knowledge graph based on the entity involved in the historical

data and the association relationship between different entities.

[0091] In the above-mentioned embodiments, the historical data is really generated data, and can reflect an objective fact. The historical data can include at least one of the social data, the transaction data, and the geographic location data, so that the historical data can depict the plurality of entities and the association relationship between the plurality of entities more richly and more stereoscopically. In this way, the knowledge graph is generated by analyzing the historical data, to ensure comprehensiveness and accuracy of the knowledge graph.

[0092] S340: Verify authenticity of the target transaction based on the transaction information, the document key information, and the knowledge graph by using a large model, to obtain an authenticity verification result.

[0093] In this specification, the large model can be a deep learning model with a large parameter quantity and a complex structure. In a training process, a prediction and generation capability of the large model is improved by learning an extremely complex pattern and feature.

[0094] In some embodiments, the large model can include a generative large language model. The generative large language model can automatically generate text associated with an input statement based on the input statement. The generative language model can include an autoencoding model or an autoregressive model. In some embodiments, the autoencoding model can be a series of models based on a transformer (a language model using an attention mechanism) technology, a series of models based on a bidirectional encoder representations from transformers (BERT) technology or another similar model, or any combination thereof. In some embodiments, the autoencoding model can be a BERT, a robustly optimized BERT pretraining approach (RoBERTa), a SpanBERT (Improving Pre-training by Representing and Predicting Spans) or another similar model, or any combination thereof. In some embodiments, the autoregressive model can be a series of models based on a generative pre-trained transformer (GPT) technology, a series of models based on a ChatGLM technology, a series of models based on an LLaMa (a universal language model using more tokens and smaller parameter sizes) technology or another similar model, or any combination thereof. In some embodiments, a large model based on the GPT technology can be ChatGPT3.5, ChatGPT4.0, etc.

[0095] A large model can be deployed on the computing device 200. The computing device 200 can verify the authenticity of the target transaction based on the transaction information, the document key information, and the knowledge graph information by using the large model, to

obtain the authenticity verification result.

[0096] FIG. 5 is a schematic flowchart of transaction authenticity verification according to an embodiment of this specification. As shown in FIG. 5, the computing device 200 can verify authenticity of the target transaction in the following manner.

[0097] (1) Perform reasoning based on the knowledge graph, to obtain reasoning information.

[0098] Reasoning can be a process of performing logical reasoning based on an existing entity and relationship information in the knowledge graph. In this specification, a reasoning process can be performing reasoning based on a reasoning rule, or can be performing reasoning based on a model. This is not limited in this specification. The computing device 200 can perform reasoning based on the knowledge graph, to obtain the reasoning information. For example, the computing device 200 learns, from the knowledge graph, that X is a father of Y and Y is a mother of Z, and obtains the following reasoning information through reasoning: X is a grandfather of Z. In this specification, the reasoning information can be information obtained by performing reasoning processing based on information in the knowledge graph. The reasoning information has a higher knowledge dimension than the information originally included in the knowledge graph, can be considered as a summary and sublimation of the original information in the knowledge graph, and is more easily understood by the large model.

[0099] In some embodiments, after the computing device 200 obtains the reasoning information based on the knowledge graph, the reasoning information can be added to the knowledge graph, to make the knowledge graph more perfect.

[0100] In some embodiments, the computing device 200 can determine, from the knowledge graph, a plurality of target entities associated with the transaction participant of the target transaction, and an association relationship between the plurality of target entities. As described above, the knowledge graph can describe the plurality of entities and the association relationship between the plurality of entities. The computing device 200 can determine, from the knowledge graph based on the transaction participant of the target transaction, the plurality of target entities associated with the transaction participant of the target transaction, and the association relationship between the plurality of target entities. For example, if the transaction participant of the target transaction includes "Tom" and "Jim", the target entity determined by the computing device 200 in the knowledge graph can include an entity associated with "Tom" (for example, an entity "Tom" and another entity connected to the entity "Tom") and an entity associated with "Jim" (for example,

an entity "Jim" and another entity connected to the entity "Jim"). It should be noted that the plurality of target entities and the association relationship between the plurality of target entities that are determined by the computing device 200 in the knowledge graph can be considered as a subgraph including the entities "Tom" and "Jim" in the knowledge graph.

[0101] The computing device 200 can obtain at least one piece of fact information based on the plurality of target entities and the association relationship between the plurality of target entities. The fact information is information directly extracted from the knowledge graph. The fact information can also be understood as part of the information based on which the knowledge graph is constructed.

[0102] Further, the computing device 200 can perform reasoning based on the at least one piece of fact information and a reasoning rule or a model, to obtain the reasoning information.

[0103] In the above-mentioned embodiments, the computing device 200 first determines, from the knowledge graph, the plurality of target entities associated with the transaction participant of the target transaction and the association relationship between the plurality of target entities, further obtains the fact information based on the plurality of target entities and the association relationship between the plurality of target entities, and performs reasoning based on the fact information, to obtain the reasoning information. In this way, only some content in the knowledge graph needs to be reasoned, and not all content in the knowledge graph needs to be reasoned, so that a calculation amount required for a reasoning process can be reduced.

[0104] (2) Prompt the large model to generate answer information corresponding to the at least one question based on the transaction information, the document key information, and the reasoning information.

[0105] The at least one question is a question used to verify the authenticity of the target transaction, or the at least one question is a question that needs to be reviewed by the review person in a process of verifying authenticity of the target transaction. The at least one question can be a preset fixed question, or can be a question dynamically determined by the computing device 300 based on an actual situation of the target transaction.

[0106] In some embodiments, before step (2), the computing device 200 can further dynamically determine the at least one question based on the actual situation of the target transaction. The at least one question can be determined in a plurality of manners. The following provides descriptions by using an example.

[0107] In some embodiments, the computing device 200 can determine the at least one question based on at least one of a transaction type corresponding to the target transaction and a document type corresponding to the transaction certificate document.

[0108] For example, the computing device 200 can determine the at least one question based on the transaction type corresponding to the target transaction. Specifically, the computing device 200 can pre-maintain a first question library. The first question library includes at least one question respectively corresponding to different transaction types. For example, content of the first question library can be shown in Table 1.

Table 1

Transaction type	Question
Transaction type A	Question Q1: What is a relationship between a remitter and a remittee?
Transaction Type B	Question Q1: What is a relationship between a remitter and a remittee? Question Q2: What is a fund source of the remitter?
...	...

[0109] In this way, the computing device 200 can query Table 1 based on the transaction type corresponding to the target transaction, to obtain at least one question. For example, if the transaction type corresponding to the target transaction is the transaction type A, it is determined that the at least one question includes the question Q1. If the transaction type corresponding to the target transaction is the transaction type B, it is determined that the at least one question includes the question Q1 and the question Q2, and so on.

[0110] For example, the computing device 200 can determine the at least one question based on the document type corresponding to the transaction certificate document. Specifically, the computing device 200 can pre-maintain a second question library. The second question library includes at least one question respectively corresponding to different document types. For example, content of the second question library can be shown in Table 2.

Table 2

Document type	Question
Document type a	Question Q1: What is a relationship between a remitter and a remittee?
Document type b	Question Q2: What is a fund source of the remitter?
...	...

[0111] In this way, the computing device 200 can query Table 2 based on the document type corresponding to the transaction certificate document, to obtain at least one question. For example, if the document type corresponding to the transaction certificate document is the document type a, it is determined that the at least one question includes the question Q1. If the document type corresponding to the transaction certificate document is the document type b, it is determined that the at least one question includes the question Q2, and so on.

[0112] For example, the computing device 200 can determine the at least one question based on the transaction type corresponding to the target transaction and the document type corresponding to the transaction certificate document. Specifically, the computing device 200 can obtain at least one first candidate question based on a transaction type query table 1 corresponding to the target transaction, and obtain at least one second candidate question based on a document type query table 2 corresponding to the transaction certificate document. The computing device 200 determines the at least one question based on the at least one first candidate question and the at least one second candidate question. For example, the at least one first candidate question and the at least one second candidate question are de-duplicated, to obtain the at least one question. Alternatively, the same question in the at least one first candidate question and the at least one second candidate question is used as the at least one question.

[0113] In the above-mentioned embodiments, the computing device 200 determines the at least one question based on the transaction type and/or the document type, so that the determined question can more accurately reflect a review priority of the target transaction, and accuracy of authenticity verification performed on the transaction by the large model is also improved.

[0114] In some embodiments, the computing device 200 can generate prompt information based on the transaction information, the document key information, the reasoning information,

and the at least one question. The prompt information can be used to prompt the large model to answer the at least one question based on the transaction information, the document key information, and the reasoning information. Further, the computing device 200 can input the prompt information into the large model, and obtain the answer information corresponding to the at least one question output by the large model.

[0115] The prompt information is an input or instructions provided to the large model, to prompt the large model to generate a specific type of output or execute a specific task. The prompt information can be part of a text string, a question, a command, or even a conversation history, and is intended to stimulate the large model to produce an output that satisfies an expectation of the user. For example, the prompt information can be "Please answer a question based on information in the following three aspects: What is a relationship between a remitter and a remittee?" Information in a first aspect includes: A remittee is Tom, a remittee is Jim, and a remittance amount is X (namely, the transaction information). Information in a second aspect includes: Tom and Jim are married (namely, the document key information). Information in the third aspect includes: Tom and Jim have a couple relationship (namely, the reasoning information). The computing device 200 inputs the prompt information into the large model, and a result of an input into the large model can be: A remitter and a remittee have a couple relationship.

[0116] In the above-mentioned embodiments, the computing device 200 generates the prompt information, to prompt the large model to answer a question. In addition, accuracy of the answer information can be improved, and transaction authenticity verification is automated, so that the review person does not need to perform manual review. In addition, transaction authenticity verification efficiency can be further improved, and training costs for the review person can be reduced.

[0117] (3) Verify authenticity of the target transaction based on the answer information corresponding to the at least one question, to obtain an authenticity verification result.

[0118] After obtaining the answer information corresponding to the at least one question, the computing device 200 can determine the authenticity verification result of the target transaction based on the answer information corresponding to the at least one question. For example, relative remittance (that is, the transaction type is relative remittance) is used as an example. It is assumed that the determined at least one question includes: What is a relationship between a remitter and a remittee? If the answer information output by the large model indicates that the remitter and the

remittee have a couple relationship, the computing device 200 can determine that the target transaction is a real transaction, in other words, the authenticity verification result of the target transaction is that verification succeeds. If the answer information output by the large model indicates that the remitter and the remittee have a non-relative relationship, the computing device 200 can determine that the target transaction is not a real transaction, in other words, the authenticity verification result of the target transaction is that verification fails.

[0119] In the above-mentioned embodiments, the computing device 200 prompts the large model to generate the answer information corresponding to the at least one question based on the transaction information, the document key information, and the reasoning information, and further determines the authenticity verification result of the target transaction based on the answer information corresponding to the at least one question. In this way, the transaction authenticity is intelligently verified through an excellent semantic understanding capability of the large model, to improve efficiency and accuracy of transaction authenticity verification.

[0120] In some embodiments, in step (1), the computing device 200 performs reasoning based on the knowledge graph, and in addition to obtaining the reasoning information, can further obtain reasoning credibility corresponding to the reasoning information. The reasoning credibility represents/reflects credibility of the reasoning information. For example, the knowledge graph describes that X is a father of Y, Y is a mother of Z, and the computing device 200 can obtain the following reasoning information after the reasoning process: X is a grandfather of Z, and can further learn that the reasoning credibility corresponding to the reasoning information as 98%.

[0121] In step (2), the computing device 200 can prompt the large model to generate the answer information corresponding to the at least one question and answer credibility corresponding to the answer information based on the transaction information, the document key information, the reasoning information, and the reasoning credibility. The answer credibility represents/reflects credibility of the answer information. In some embodiments, the answer credibility and the reasoning credibility can be positively correlated. For example, when the reasoning credibility is high, the answer credibility is also high, and when the reasoning credibility is low, the answer credibility is also low.

[0122] In step (3), the computing device 200 can verify the authenticity of the target transaction based on the answer information corresponding to the at least one question and the answer credibility corresponding to the answer information, to obtain thr authenticity verification

result. That is, when performing authenticity verification on the target transaction, the computing device 200 not only considers the answer information of the large model for the at least one question, but also considers the answer credibility corresponding to the answer information. For example, the relative remittance (namely, the transaction type is a relative remittance) as an example. It is assumed that the at least one question includes: What is a relationship between a remitter and a remittee? If the answer information corresponding to the question represents that the remitter and the remittee have a couple relationship, and the answer credibility corresponding to the answer information is 98%, the computing device 200 determines that the authenticity verification result of the target transaction is that verification succeeds. If the answer information corresponding to the question represents that the remitter and the remittee have a couple relationship, and the answer credibility corresponding to the answer information is 30%, the computing device 200 determines that the authenticity verification result of the target transaction is that verification fails.

[0123] In the above-mentioned embodiments, when the computing device 200 performs reasoning based on the knowledge graph, not only reasoning information can be obtained, but also reasoning credibility corresponding to the reasoning information can be obtained. Therefore, the computing device 200 can prompt the large model to answer the at least one question, and can further refer to the reasoning credibility corresponding to the reasoning information, to obtain answer credibility corresponding to the answer information of the at least one question. Further, when determining the authenticity verification result of the target transaction, the computing device 200 can consider the answer credibility corresponding to the answer information, to help improve accuracy of the authenticity verification result of the target transaction.

[0124] The following describes an execution manner of the transaction authenticity verification method P300.

[0125] In some embodiments, the transaction authenticity verification method P300 can be used to perform authenticity verification on a real-time transaction. That is, when receiving the transaction request of the target transaction, the service platform triggers in real time the transaction authenticity verification method P300.

[0126] For example, with reference to FIG. 1, after detecting that the user 110 initiates the target transaction operation, the terminal device 120 receives the target transaction request. The terminal device 120 can obtain the transaction information of the target transaction based on the

transaction request, can further obtain the transaction certificate document uploaded by the user 110 for the target transaction, and extract the document key information from the transaction certificate document. Further, the terminal device 120 obtains the knowledge graph pre-constructed based on the fact data, and verify the authenticity of the target transaction based on the transaction information, the document key information, and the knowledge graph by using the large model, to obtain the authenticity verification result. If the authenticity verification result indicates that the target transaction is not a real transaction, the terminal device 120 intercepts the target transaction. If the authenticity verification result represents that the target transaction is a real transaction, the terminal device 120 releases the target transaction.

[0127] For another example, with reference to FIG. 1, after detecting an operation of initiating the target transaction by the user 110, the terminal device 120 can require the user 110 to upload the transaction certificate document corresponding to the target transaction. The terminal device 120 sends the transaction request for the target transaction to the server 130, and sends the transaction certificate document corresponding to the target transaction to the server 130. Therefore, the server 130 can receive the transaction request of the target transaction, and obtain the transaction information of the target transaction based on the transaction request. The server 130 can further receive the transaction certificate document corresponding to the target transaction, and extract the document key information from the transaction certificate document. Further, the server 130 obtains the knowledge graph pre-constructed based on the fact data, and verify the authenticity of the target transaction based on the transaction information, the document key information, and the knowledge graph by using the large model, to obtain the authenticity verification result. If the authenticity verification result indicates that the target transaction is not a real transaction, the server 130 indicates the terminal device 120 to intercept the target transaction. If the authenticity verification result represents that the target transaction is a real transaction, the server 130 indicates the terminal device 120 to release the target transaction. Correspondingly, the terminal device 120 can display an execution result of the target transaction to the user 110 on an interaction page.

[0128] In some embodiments, the transaction authenticity verification method P300 can be used to perform authenticity verification on a non-real-time transaction. That is, after receiving the transaction request of the target transaction, the service platform can request the user to upload the transaction certificate document corresponding to the target transaction. The service platform can

generate the transaction authenticity verification task corresponding to the target transaction based on the transaction information and the transaction certificate document of the target transaction, and add the transaction authenticity verification task to the task queue. When performing authenticity on the target transaction, the service platform obtains the transaction authenticity verification task corresponding to the target transaction from the task queue, to trigger authenticity verification on the target transaction.

[0129] For example, the server 130 obtains a transaction authenticity verification task corresponding to the target transaction from the task queue. The server 130 can obtain the transaction information of the target transaction and the transaction certificate document corresponding to the target transaction through parsing from the transaction authenticity verification task, and can further obtain the document key information from the transaction certificate document. Further, the server 130 obtains the knowledge graph pre-constructed based on the fact data, and verify the authenticity of the target transaction based on the transaction information, the document key information, and the knowledge graph by using the large model, to obtain the authenticity verification result. If the authenticity verification result indicates that the target transaction is not a real transaction, the server 130 indicates the terminal device 120 to intercept the target transaction. If the authenticity verification result represents that the target transaction is a real transaction, the server 130 indicates the terminal device 120 to release the target transaction. Correspondingly, the terminal device 120 pushes notification information to the user 110, so that the user 110 learns of the execution result of the target transaction in a timely manner.

[0130] In conclusion, in the transaction authenticity verification method and system, and the storage medium provided in this specification, the computing device 200 can verify the authenticity of the target transaction based on the transaction information of the target transaction, the document key information in the transaction certificate document corresponding to the target transaction, and the pre-constructed knowledge graph by using the large model, to obtain the authenticity verification result. The above-mentioned solution implements automatic authenticity verification on the target transaction by using the large model, to improve verification efficiency, so that a service system can quickly release a transaction and reduce a user waiting time. Because no review person needs to perform manual review, training costs of the review person can be further reduced. Further, in the technical solutions, the large model and the knowledge graph are

combined. The knowledge graph can improve a semantic understanding capability of the large model. In addition, the knowledge graph provides the large model with fact information related to a transaction participant of the target transaction, so that the large model can better understand a relationship with the transaction participant of the target transaction. Roles of the knowledge graph in the two aspects can improve accuracy and reliability of performing authenticity verification on the target transaction by the large model.

[0131] In addition, the knowledge graph can be used as a prior knowledge of the large model, to reduce a requirement of the large model for pre-training, and reduce model training costs. In a new transaction scenario, even in a case in which training data in the new transaction scenario cannot be obtained, and consequently, the large model cannot be adequately trained, the knowledge graph can help the large model to be quickly applied to the new transaction scenario, to avoid a cold start. Content of the knowledge graph can be updated periodically or occasionally. This dynamic feature enables the knowledge graph to provide latest knowledge for the large model, to improve accuracy of answering a question by the large model.

[0132] Another aspect of this specification provides a non-transitory storage medium, storing at least one instruction set, to perform transaction authenticity verification. When the at least one instruction set is executed by a processor, the at least one instruction set instructs the processor to implement steps of the transaction authenticity verification method P300 described in this specification. In some possible implementations, aspects of this specification can further be implemented in a form of a program product, including program code. When the program product runs on a computing device 200, the program code is used to enable the computing device 200 to perform steps of the transaction authenticity verification method P300 described in this specification. The program product configured to implement the foregoing method can use a portable compact disc read-only memory (CD-ROM) that includes program code, and can run on the computing device 200. However, the program product in this specification is not limited thereto. In this specification, a readable storage medium can be any tangible medium that includes or stores a program, and the program can be used by or in combination with an instruction execution system. The program product can be any combination of one or more readable media. The readable medium can be a readable signal medium or a readable storage medium. The readable storage medium can be, for example, an electrical system, apparatus, or device, a magnetic system, apparatus, or device, an optical system, apparatus, or device, an electromagnetic system, apparatus,

or device, an infrared system, apparatus, or device, or a semiconductor system, apparatus, or device, or any combination thereof. More specific examples of the readable storage medium include: an electrical connection including one or more conducting wires, a portable disk, a hard disk, a random access memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory (EPROM or flash memory), an optical fiber, a portable compact disc read-only memory (CD-ROM), an optical storage component, a magnetic storage component, or any proper combination thereof. The computer-readable storage medium can include a data signal propagated in a baseband or as part of a carrier, and carries readable program code. The propagated data signal can be in a plurality of forms, and includes but is not limited to an electromagnetic signal, an optical signal, or any proper combination thereof. The readable storage medium can further be any readable medium other than the readable storage medium, and the readable medium can be used to send, propagate, or transmit a program used by or in combination with an instruction execution system, apparatus, or component. The program code included in the readable storage medium can be transmitted in any proper medium, including but not limited to a wireless medium, a wired medium, optical cable, an RF medium, or any proper combination thereof. Program code for performing an operation of this specification can be written in any combination of one or more program design languages. The program design language includes an object-oriented program design language, for example, Java or C++, and further includes a conventional procedural program design language, for example, "C" language, or a similar program design language. The program code can be completely executed on the computing device 200, partially executed on the computing device 200, executed as an independent software package, partially executed on the computing device 200 and partially executed on a remote computing device, or completely executed on a remote computing device.

[0133] Specific embodiments of this specification are described above. Other embodiments fall within the scope of the appended claims. In some cases, the actions or steps described in the claims can be performed in an order different from that in the embodiments, and the desired results can still be achieved. In addition, the process depicted in the accompanying drawings does not necessarily need a particular order or consecutive order to achieve the desired results. In some implementations, multitasking and parallel processing are possible or may be advantageous.

[0134] In conclusion, after reading the detailed disclosure, a person skilled in the art can understand that the detailed disclosure can be presented only in an example manner, and can

impose no limitation. Although it is not explicitly stated here, a person skilled in the art can understand that the requirements of this specification include various proper changes, improvements, and modifications to the embodiments. These changes, improvements, and modifications are intended to be presented in this specification, and fall within the spirit and scope of the example embodiments of this specification.

[0135] In addition, some terms in this specification are used to describe the embodiments of this specification. For example, "one embodiment", "an embodiment", and/or "some embodiments" mean that particular features, structures, or characteristics described with reference to the embodiments can be included in at least one embodiment of this specification. Therefore, it can be emphasized and understood that two or more of "an embodiment", "one embodiment", or "alternative embodiments" referred in parts of this specification do not necessarily indicate the same embodiment. In addition, particular features, structures, or characteristics can be properly combined in one or more embodiments of this specification.

[0136] It should be understood that in the above-mentioned descriptions of the embodiments of this specification, to help understand a feature, for the purpose of simplifying this specification, various features are combined in a single embodiment, accompanying drawing, or description thereof in this specification. However, this does not mean that the combination of these features is necessary. It is entirely possible for a person skilled in the art to mark some devices and understand the devices as separate embodiments when reading this specification. In other words, the embodiments in this specification can also be understood as an integration of a plurality of secondary embodiments. Content of each secondary embodiment is also true when features are less than all features in one of the above-mentioned disclosed embodiments.

[0137] Each patent, patent application, publication of a patent application, and other materials, for example, articles, books, instructions, publications, documents, and products, that are cited in this specification and that are other than any document that is inconsistent or conflict with this document or that imposes limiting impact on the widest scope of the claims can be incorporated here by reference and used for all purposes now or later associated with this document. In addition, the term in this document shall prevail when there is any inconsistency or conflict between the description, definition and/or use of a related term in any material and the description, definition and/or use of a related term in this document.

[0138] Finally, it should be understood that the principles of the implementation solutions of

this specification are described in the implementation solutions of the application disclosed in this specification. Other modified embodiments also fall within the scope of this specification. Therefore, the embodiments disclosed in this specification are merely examples and not limitations. A person skilled in the art can use an alternative configuration according to the embodiments of this specification to implement the application in this specification. Therefore, the embodiments of this specification are not limited to the embodiments accurately described in the application.

CLAIMS

What is claimed is:

1. A transaction authenticity verification method, comprising:

obtaining transaction information of a target transaction;

obtaining a transaction certificate document corresponding to the target transaction, and extracting document key information from the transaction certificate document;

obtaining a knowledge graph pre-constructed based on fact data, wherein the knowledge graph represents a plurality of entities and an association relationship between the plurality of entities, and the plurality of entities comprise at least an entity corresponding to a transaction participant of the target transaction; and

verifying authenticity of the target transaction based on the transaction information, the document key information, and the knowledge graph by using a large model, to obtain an authenticity verification result.

2. The method according to claim 1, wherein the verifying authenticity of the target transaction based on the transaction information, the document key information, and the knowledge graph by using a large model, to obtain an authenticity verification result comprises:

performing reasoning based on the knowledge graph, to obtain reasoning information;

prompting the large model to generate answer information corresponding to at least one question based on the transaction information, the document key information, and the reasoning information, wherein the at least one question is a question used to verify the authenticity of the target transaction; and

verifying authenticity of the target transaction based on the answer information corresponding to the at least one question, to obtain an authenticity verification result.

3. The method according to claim 2, wherein the verifying authenticity of the target transaction based on the transaction information, the document key information, and the knowledge graph by using a large model, to obtain an authenticity verification result further comprises:

determining the at least one question based on at least one of a transaction type corresponding to the target transaction and a document type corresponding to the transaction certificate document.

4. The method according to claim 2, wherein the performing reasoning based on the

knowledge graph, to obtain reasoning information comprises:

determining, from the knowledge graph, a plurality of target entities associated with a transaction participant of the target transaction, and an association relationship between the plurality of target entities;

obtaining at least one piece of fact information based on the plurality of target entities and the association relationship between the plurality of target entities; and

performing reasoning based on the at least one piece of fact information, to obtain the reasoning information.

5. The method according to claim 2, wherein the prompting the large model to generate answer information corresponding to the at least one question based on the transaction information, the document key information, and the reasoning information comprises:

generating prompt information based on the transaction information, the document key information, the reasoning information, and the at least one question, wherein the prompt information is used to prompt the large model to answer the at least one question based on the transaction information, the document key information, and the reasoning information; and

inputting the prompt information into the large model, and obtaining the answer information that corresponds to the at least one question and that is output by the large model.

6. The method according to claim 2, wherein

the performing reasoning based on the knowledge graph, to obtain reasoning information comprises: performing reasoning based on the knowledge graph, to obtain the reasoning information and reasoning credibility corresponding to the reasoning information;

the prompting the large model to generate answer information corresponding to at least one question based on the transaction information, the document key information, and the reasoning information comprises: prompting the large model to generate the answer information corresponding to the at least one question and answer credibility corresponding to the answer information based on the transaction information, the document key information, the reasoning information, and the reasoning credibility; and

the verifying authenticity of the target transaction based on the answer information corresponding to the at least one question, to obtain an authenticity verification result comprises: verifying the authenticity of the target transaction based on the answer information corresponding to the at least one question and the answer credibility corresponding to the answer information, to

obtain the authenticity verification result.

7. The method according to claim 1, wherein the knowledge graph is constructed in the following manner:

obtaining historical data generated in a historical time period;

analyzing the historical data, to obtain an entity involved in the historical data and an association relationship between different entities; and

generating the knowledge graph based on the entity involved in the historical data and the association relationship between different entities.

8. The method according to claim 7, wherein the historical data comprises at least one of social data, transaction data, and geographic location data.

9. The method according to claim 1, wherein the extracting document key information from the transaction certificate document comprises:

performing text recognition on the transaction certificate document, to obtain a text recognition result;

determining a document type corresponding to the transaction certificate document; and

performing information extraction on the text recognition result based on the document type corresponding to the transaction certificate document, to obtain the document key information.

10. The method according to claim 9, wherein the performing information extraction on the text recognition result based on the document type corresponding to the transaction certificate document, to obtain the document key information comprises:

determining a target information extraction model corresponding to the document type from a plurality of information extraction models; and

performing information extraction on the text recognition result by using the target information extraction model, to obtain the document key information in the transaction certificate document.

11. The method according to claim 1, wherein

the obtaining transaction information of a target transaction comprises: receiving a transaction request of the target transaction, and obtaining the transaction information of the target transaction based on the transaction request; and

after the authenticity verification result is obtained, the method further comprises: releasing the target transaction based on the authenticity verification result, or intercepting the target

transaction.

12. A transaction authenticity verification system, comprising:

at least one storage medium, storing at least one instruction set, to perform transaction authenticity verification; and

at least one processor, communicatively connected to the at least one storage medium, wherein

when the system runs, the at least one processor reads the at least one instruction set, and performs the following operations based on an indication of the at least one instruction set:

obtaining transaction information of a target transaction;

obtaining a transaction certificate document corresponding to the target transaction, and extracting document key information from the transaction certificate document;

obtaining a knowledge graph pre-constructed based on fact data, wherein the knowledge graph represents a plurality of entities and an association relationship between the plurality of entities, and the plurality of entities comprise at least an entity corresponding to a transaction participant of the target transaction; and

verifying authenticity of the target transaction based on the transaction information, the document key information, and the knowledge graph by using a large model, to obtain an authenticity verification result.

13. The system according to claim 12, wherein to verify the authenticity of the target transaction based on the transaction information, the document key information, and the knowledge graph by using the large model, to obtain the authenticity verification result, the at least one processor performs the following operations:

performing reasoning based on the knowledge graph, to obtain reasoning information;

prompting the large model to generate answer information corresponding to at least one question based on the transaction information, the document key information, and the reasoning information, wherein the at least one question is a question used to verify the authenticity of the target transaction; and

verifying authenticity of the target transaction based on the answer information corresponding to the at least one question, to obtain an authenticity verification result.

14. The system according to claim 13, wherein to perform reasoning based on the knowledge graph, to obtain the reasoning information, the at least one processor performs the following

operations:

determining, from the knowledge graph, a plurality of target entities associated with a transaction participant of the target transaction, and an association relationship between the plurality of target entities;

obtaining at least one piece of fact information based on the plurality of target entities and the association relationship between the plurality of target entities; and

performing reasoning based on the at least one piece of fact information, to obtain the reasoning information.

15. The system according to claim 13, wherein to prompt the large model to generate the answer information corresponding to the at least one question based on the transaction information, the document key information, and the reasoning information, the at least one processor performs the following operations:

generating prompt information based on the transaction information, the document key information, the reasoning information, and the at least one question, wherein the prompt information is used to prompt the large model to answer the at least one question based on the transaction information, the document key information, and the reasoning information; and

inputting the prompt information into the large model, and obtaining the answer information that corresponds to the at least one question and that is output by the large model.

16. The system according to claim 13, wherein

to perform reasoning based on the knowledge graph, to obtain the reasoning information, the at least one processor performs the following operations: performing reasoning based on the knowledge graph, to obtain the reasoning information and reasoning credibility corresponding to the reasoning information;

to prompt the large model to generate the answer information corresponding to the at least one question based on the transaction information, the document key information, and the reasoning information, the at least one processor performs the following operations: prompting the large model to generate the answer information corresponding to the at least one question and answer credibility corresponding to the answer information based on the transaction information, the document key information, the reasoning information, and the reasoning credibility; and

to verify the authenticity of the target transaction based on the answer information corresponding to the at least one question, to obtain the authenticity verification result, the at least

one processor performs the following operations: verifying the authenticity of the target transaction based on the answer information corresponding to the at least one question and the answer credibility corresponding to the answer information, to obtain the authenticity verification result.

17. The system according to claim 12, wherein the knowledge graph is constructed in the following manner:

obtaining historical data generated in a historical time period;

analyzing the historical data, to obtain an entity involved in the historical data and an association relationship between different entities; and

generating the knowledge graph based on the entity involved in the historical data and the association relationship between different entities.

18. The system according to claim 17, wherein the historical data comprises at least one of social data, transaction data, and geographic location data.

19. The system according to claim 12, wherein to extract the document key information from the transaction certificate document, the at least one processor performs the following operations:

performing text recognition on the transaction certificate document, to obtain a text recognition result;

determining a document type corresponding to the transaction certificate document; and

performing information extraction on the text recognition result based on the document type corresponding to the transaction certificate document, to obtain the document key information.

20. A computer-readable non-transitory storage medium, wherein the computer-readable non-transitory storage medium stores at least one instruction set, and when the at least one instruction set is executed by at least one processor, the method according to any one of claims 1 to 11 is implemented.