

IDENTITY VERIFICATION METHOD AND SYSTEM, STORAGE MEDIUM AND CHIP

TECHNICAL FIELD

[0001] The present application relates to the field of computer technologies, and in particular, to an identity verification method and system, a storage medium and a chip.

BACKGROUND

[0002] With rapid development of express delivery industries, in order to better ensure security of express deliveries from sources, China has officially initiated real-name registration for the express deliveries. To meet needs of real-name shipping, a courier needs to perform identity verification on a user, when providing a shipping service to the user. In a current scenario of express delivery shipping, if the user has previously performed a real-name authentication on a logistics company platform, the user submits a shipping order online, and the courier directly completes the identity verification for the user through the logistics company platform when providing the shipping service to the user; and if the user has not performed the real-name authentication on the logistics company platform, the courier needs to perform verification on identity information presented by the user. In addition, when the user needs to ship valuable items, even if the user has previously performed the real-name authentication on the logistics company platform, the courier still needs to perform the verification on the identity information presented by the user again when receiving the items.

[0003] When the courier needs to perform the verification on the identity information presented by the user, a time cost of the courier will be greatly increased. Moreover, whether the user performs the real-name authentication on the logistics company platform or presents the identity information to the courier, a leakage risk of user information will be increased. Therefore, how to improve security of the user information and realize the identity verification for the user has become an urgent technical problem that needs to be solved.

SUMMARY

[0004] Embodiments of the present application provide an identity verification method and system, a storage medium and a chip, which can realize identity authentication for a user and reduce a leakage risk of information.

[0005] In a first aspect, the embodiments of the present application provide an identity verification method, applied to an identity verification system, where the identity verification system includes a logistics management platform, a plurality of courier terminals and a decentralized identity system, and the method includes: sending, by the logistics management platform or a target courier terminal, an identity verification request to the decentralized identity system, where the identity verification request includes a first decentralized identifier DID and a first verifiable claim VC document, and the target courier terminal is one of the plurality of courier terminals; performing, by the decentralized identity system, identity verification on a user based on the identity verification request to obtain an identity verification result; and in a case that the identity verification result is successfully verified, performing, by the decentralized identity system, verification on order information to obtain an order verification result, and sending, by the decentralized identity system, the order verification result to the target courier terminal.

[0006] In a second aspect, the embodiments of the present application provide an identity verification system, including a logistics management platform, a plurality of courier terminals and a decentralized identity system, the logistics management platform is configured to execute steps executed by the logistics management platform in the method described in the above first aspect, one of the plurality of courier terminals is configured to execute steps executed by the target courier terminal in the method described in the above first aspect, and the decentralized identity system is configured to execute steps executed by the decentralized identity system in the method described in the above first aspect.

[0007] In a third aspect, the embodiments of the present application provide a computer-readable storage medium, where the computer-readable storage medium stores a computer program or an instruction, when a computer reads and executes the computer program or the instruction, the computer is caused to execute the method described in the above first aspect.

[0008] In a fourth aspect, the embodiments of the present application provide a chip, including a processor configured to invoke and run a computer program from a memory, causing a computer device equipped with the chip to execute the method described in the above first aspect.

[0009] In the identity verification method provided by the present application, the decentralized identity system is configured to perform identity verification and order information verification. The identity verification is configured to determine that a user is a real user, that is, the user and a person in reality are in a one-to-one correspondence. The order information verification is configured to determine legality of an order, that is, the order

information is ordered by the user and processes legal attributes. Since both the identity verification and the order information verification are completed by the decentralized identity system, the user only needs to complete real-name authentication in the decentralized identity system, and the user does not need to perform the real-name authentication in the logistics management platform, nor does the user need to present identity information to a courier, which may maximally ensure security of the identity information of the user, thereby realizing the identity authentication for the user and reducing the leakage risk of the information.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] To more clearly illustrate technical solutions in embodiments of the present application, the accompanying drawings that are required to be used in description of the embodiments or the related technologies will be briefly introduced below. Apparently, the accompanying drawings in the following description show only some embodiments of the present application. As for those with ordinary skill in the art, other drawings may also be obtained according to these accompanying drawings without creative work.

[0011] FIG. 1 is a schematic diagram of a scenario of an identity verification system provided by an embodiment of the present application.

[0012] FIG. 2 is a principle diagram of applying a decentralized identity provided by an embodiment of the present application.

[0013] FIG. 3 is a schematic interaction diagram of a process of real-name registration in a decentralized identity system provided by an embodiment of the present application.

[0014] FIG. 4 is a schematic interaction diagram of an identity verification method provided by an embodiment of the present application.

[0015] FIG. 5 is a schematic interaction diagram of an identity verification method provided by another embodiment of the present application.

[0016] FIG. 6 is a schematic internal structural diagram of a computer device provided by an embodiment of the present application.

[0017] FIG. 7 is a schematic internal structural diagram of a storage medium provided by an embodiment of the present application.

DETAILED DESCRIPTION OF THE EMBODIMENTS

[0018] To meet needs of real-name shipping, a courier needs to perform identity verification on a user, when providing a shipping service to the user. Whether the user performs real-name

authentication on a logistics company platform or presents identity information to the courier, a leakage risk of user information will be increased. Therefore, how to achieve the identity verification for the user and improve security of the user information (or how to achieve identity authentication for the user and reduce the leakage risk of the information) has become an urgent technical problem that needs to be solved.

[0019] FIG. 1 is a schematic diagram of a scenario of an identity verification system provided by an embodiment of the present application. As shown in FIG. 1, the scenario includes an identity verification system 100 and a user terminal 200. The identity verification system 100 includes a logistics management platform 110, a plurality of courier terminals 121, 122, 123...12m and a decentralized identity system 130. The logistics management platform 110 is communicatively connected to the user terminal 200, the plurality of courier terminals 121, 122, 123...12m and the decentralized identity system 130, respectively, and the plurality of courier terminals 121, 122, 123...12m are communicatively connected to the decentralized identity system 130.

[0020] Exemplarily, the logistics management platform 110 interacts with the user terminal 200, the plurality of courier terminals 121, 122, 123... 12m, and the decentralized identity system 130. For example, the logistics management platform 110 receives a login request sent by the user terminal 200 and performs login verification on a user based on the login request; the logistics management platform 110 receives order information sent by the user terminal 200, determines a target courier terminal 12x from the plurality of courier terminals 121, 122, 123...12m based on the order information, and sends the order information to the target courier terminal 12x, that is, assigning an order to the target courier terminal 12x; after receiving the order information, the target courier terminal 12x sends an identity verification request to the decentralized identity system 130, and the decentralized identity system 130 performs identity verification on the user based on the identity verification request to obtain an identity verification result; in a case that the identity verification result is successfully verified, the target courier terminal 12x sends an order verification request to the decentralized identity system 130; and after receiving the order verification request, the decentralized identity system 130 performs verification on the order information based on the order verification request to obtain an order verification result, and sends the order verification result to the target courier terminal 12x.

[0021] In addition to the above-mentioned case where the target courier terminal 12x sends the identity verification request to the decentralized identity system 130, the identity

verification request may also be sent by the logistics management platform 110 to the decentralized identity system 130.

[0022] It may be understood that, the logistics management platform 110 is an internal management system of a logistics company, for example, the logistics management platform 110 may be a server that provides a logistics service for the logistics company; the plurality of courier terminals 121, 122, 123...12m are terminal devices used by couriers of the logistics company, for example, the plurality of courier terminals 121, 122, 123...12m may be handheld devices (such as mobile phones or scanners), vehicle-mounted devices, wearable devices, or the like; the decentralized identity system 130 is a platform that performs real-name authentication and the identity verification on the user, and performs order verification, for example, the decentralized identity system 130 may include a server and a blockchain for realizing a decentralized identity function; and the user terminal 200 is a terminal device used by the user who wishes to ship items.

[0023] It should be understood that in the embodiments of the present application, the user may utilize the user terminal 200 to perform real-name registration in the decentralized identity system 130, eliminating needs for the real-name registration in the logistics management platform 110; and the decentralized identity system 130 performs the identity verification on the user terminal 200, thereby avoiding problems of a courier spending excessive time on the identity verification and the leakage of identity information of the user.

[0024] Furthermore, the decentralized identity system 130 adopts a decentralized identity, which is also known as a Decentralized Identity (DID). The decentralized identity based on a blockchain has characteristics such as ensuring data authenticity and credibility, protecting user privacy and security, and strong portability.

[0025] For ease of understanding, before the decentralized identity system 130 is introduced in the embodiments of the present application, an exemplary illustration of a principle of the decentralized identity is provided below with reference to FIG. 2.

[0026] FIG. 2 is a principle diagram of applying a decentralized identity provided by an embodiment of the present application, mainly showing a registration or verification process. As shown in FIG. 2, in an application of the decentralized identity, participating entities include an issuer 21, a holder 22, a verifier 23, a DID registration system (for example, a blockchain node) 24, and a credential storage platform (for example, a decentralized storage node) 25. A verifiable credential (VC) is verifiable information circulated among various entities, and the VC provides a specification to describe certain attributes possessed by the entities, thereby enabling evidence-based trust. The holder 22 may prove credibility of its certain attributes to

other entities (such as the verifier 23) through the VC. A DID (that is, a decentralized identifier) is a string in a specific format and globally unique, which is used for representing a decentralized identity of the holder.

[0027] It should be understood that the issuer 21 possesses user data and can issue (or promulgate) a corresponding VC to the holder 22. For example, the issuer may be a government department, a public security organ, an educational institution, and so on. The holder 22 is a possessor of the VC, and any entity may assume this role. The verifier 23 is responsible for receiving the VC presented by the holder 22, and the verifier 23 performs verification on the VC, and provides a corresponding service for the holder 22 after the verification passes. The blockchain node 24 is responsible for verification and maintenance of data information on a chain. For example, the issuer 21 and the verifier 23 perform verification on the VC on the chain, or the holder 22 registers an identity on the chain. The decentralized storage node 25 is responsible for verification and maintenance of data information on-chain and off-chain. For example, the issuer 21 promulgates/updates/revokes user data to the decentralized storage node 25, or the holder 22 authorizes/stores the user data.

[0028] The decentralized identity system 130 in the embodiments of the present application is set up based on a principle of a decentralized identity in FIG. 2. As shown in FIG. 1, the decentralized identity system 130 in the embodiments of the present application includes an identity authentication server 132, a Certification Authority (CA) server 131, and a blockchain 133. The identity authentication server 132, the CA server 132, and the blockchain 133 are all communicatively connected with each other. It may be learned from FIG. 1 that the decentralized identity system 130 is communicatively connected to the logistics management platform 110 and the plurality of courier terminals 121, 122, 123...12m through the identity authentication server 132, respectively. For example, the logistics management platform 110 or the target courier terminal 12x sends the identity verification request to the identity authentication server 132. The blockchain 133 includes a plurality of nodes 1, 2, 3...n, and a decentralized identity is achieved through the plurality of nodes 1, 2, 3...n. Decentralization involves distributing data across the plurality of nodes 1, 2, 3...n, and the more the number of the plurality of nodes 1, 2, 3...n there are, the higher the security of the data will be. The blockchain node 24 in FIG. 2 may be understood as any node x in the blockchain 133 in FIG. 1.

[0029] It may be understood that the identity authentication server 132 may be a single server or a server cluster composed of a plurality of servers. Similarly, the CA server 131 may be a single server or a server cluster composed of a plurality of servers.

[0030] To facilitate a clearer understanding of roles of components within a decentralized identity system, an exemplary illustration of a real-name registration (also known as real-name authentication) process for a user in the decentralized identity system is provided below with reference to FIG. 1 and FIG. 3. FIG. 3 is a schematic interaction diagram of a process of real-name registration in a decentralized identity system provided by an embodiment of the present application. As shown in FIG. 3, the real-name authentication process includes following steps S301 to S309. A user terminal mentioned in the steps S301 to S309 is the user terminal 200 in FIG. 1, an identity authentication server mentioned in the steps S301 to S309 is the identity authentication server 132 in FIG. 1, a CA server mentioned in the steps S301 to S309 is the CA server 131 in FIG. 1, and a blockchain mentioned in the steps S301 to S309 is the blockchain 133 in FIG. 1.

[0031] S301: inputting, by a user, real-name registration information in the user terminal.

[0032] The real-name registration information may also be called real-name authentication information, and the real-name registration information includes identity information of the user. For example, the identity information of the user may be an ID number of the user, fingerprint information of the user, facial recognition information of the user, or the like.

[0033] S302: sending, by the user terminal, a real-name registration request to the identity authentication server based on the real-name registration information.

[0034] S303: generating, by the identity authentication server, a second DID and a second VC document corresponding to the user based on the real-name registration request.

[0035] The second DID and the second VC document correspond to the user, that is, the second DID and the second VC document may be served as digital identity information of the user. Subsequent order verification and identity verification are realized by verifying the second DID and the second VC document.

[0036] It should be understood that, unless otherwise stated, the VC document in the embodiments of the present application is the verifiable credential (VC) shown in FIG. 2.

[0037] In some embodiments, the real-name registration information may be encrypted and stored in the identity authentication server. In addition, a hash value of the real-name registration information may be uploaded to the blockchain for storage, and a hash algorithm may use sha256, sm3, or the like.

[0038] S304: sending, by the identity authentication server, a key request to the CA server.

[0039] S305: generating, by the CA server, a second public key and a second private key based on the key request.

[0040] The second public key is a public key corresponding to the user, and the second private key is a private key corresponding to the user.

[0041] It should be understood that the second private key and the second public key may be used for the subsequent order verification and identity verification, that is, the order verification and the identity verification may be performed using private key signing and public key signature verification, which is simple and easy to apply.

[0042] S306: sending, by the CA server, the second public key and the second private key to the identity authentication server.

[0043] S307: storing, by the identity authentication server, the second public key, the second DID, and the second VC document.

[0044] S308: returning, by the identity authentication server, the second private key, the second DID, and the second VC document to the user terminal.

[0045] S309: uploading, by the identity authentication server, the second public key, the second DID, and the second VC document to the blockchain.

[0046] The second private key may only be saved by the user terminal, and the second DID and the second VC document may also be saved by the user terminal. The second public key, the second DID, and the second VC document are saved by the identity authentication server and/or the blockchain.

[0047] It should be understood that when the second public key, the second DID and the second VC document are stored by the identity authentication server and the blockchain, a mapping relationship between the second DID and the second VC document, a mapping relationship between the second DID and the second public key, or the like are also stored by the identity authentication server and the blockchain.

[0048] For example, during the subsequent order verification or identity verification, the second public key and/or the second VC document may be found by the identity authentication server or the blockchain through the second DID, thereby realizing the verification.

[0049] After the user completes the real-name registration in the decentralized identity system, the second public key, the second private key, the second DID, and the second VC document are utilized by the identity verification system to realize the identity verification and the order verification for the user. Since identity information of the user does not need to be presented to the logistics management platform and the courier terminal throughout the process, the leakage of the identity information of the user may be avoided.

[0050] Based on the identity verification system provided in the above embodiments of the present application, the present application provides an identity verification method. FIG. 4 is

a schematic interaction diagram of an identity verification method provided by an embodiment of the present application. As shown in FIG. 4, the method may include steps S401 to S411. Following will illustrate each step in detail with reference to FIG. 4.

[0051] S401: receiving, by the logistics management platform, a login request sent by the user terminal, the login request including a first DID and a first VC document.

[0052] The login request sent by the user terminal is generated by the user terminal based on the first DID and the first VC document input by the user.

[0053] S402: generating, by the logistics management platform, an identity verification request based on the first DID and the first VC document.

[0054] S403: sending, by the logistics management platform, the identity verification request to the decentralized identity system, the identity verification request including the first DID and the first VC document.

[0055] S404: performing, by the decentralized identity system, identity verification on the user based on the identity verification request to obtain an identity verification result.

[0056] In some embodiments, the performing, by the decentralized identity system, the identity verification on the user based on the identity verification request may include following steps: determining, by the decentralized identity system, a target VC document corresponding to the first DID based on the first DID; and comparing, by the decentralized identity system, the target VC document with the first VC document to determine the identity verification result.

[0057] It should be understood that the DID and the VC document stored in the decentralized identity system are in a one-to-one correspondence, and the user corresponding to the DID and the VC document is a user who has completed the real-name registration in the decentralized identity system. Therefore, after the first DID is obtained by the decentralized identity system, if the target VC document corresponding to the first DID is found, and the target VC document is the same as the first VC document, the identity verification of the user is successful; and if the target VC document corresponding to the first DID is not found, or the found target VC document is different from the first VC document, the identity verification of the user is a failure.

[0058] In some other embodiments, the performing, by the decentralized identity system, the identity verification on the user based on the identity verification request may include following steps: performing, by the decentralized identity system, signature verification on the first VC document using its own public key to obtain the identity verification result. When the VC document corresponding to the user is generated by the decentralized identity system, the decentralized identity system performs an electronic signature on the VC document using its

own private key. When the first VC document is received by the decentralized identity system, the decentralized identity system performs the signature verification on first VC document using its own public key, if the signature verification passes, it proves that the first VC document is the VC document generated by the decentralized identity system, that is, the identity verification of the user is successful; and if the signature verification fails, it proves that the first VC document is not generated by the decentralized identity system, that is, the identity verification of the user is a failure.

[0059] S405: sending, by the decentralized identity system, the identity verification result as a login verification result to the logistics management platform.

[0060] S406: in a case of successful login verification, receiving, by the logistics management platform, order information sent by the user terminal.

[0061] It should be understood that the order information sent by the user terminal is obtained by the user filling in the order information in the user terminal. The order information sent by the user terminal to the logistics management platform is order information that has been electronically signed using the first private key of the user stored in the user terminal. An electronic signature technology is a mature related technology, and details are not described herein again.

[0062] S407: determining, by the logistics management platform, a target courier terminal from the plurality of courier terminals based on the order information.

[0063] S408: sending, by the logistics management platform, the order information to the target courier terminal.

[0064] It should be understood that the target courier terminal is a terminal device used by a courier who may receive the order. In general, the order information may include a shipping address, and the logistics management platform determines a courier corresponding to the shipping address based on the shipping address, thereby determining the target courier terminal.

[0065] Exemplarily, each courier has its own service area, and by determining which courier's service area the shipping address is in, a target courier is determined. The courier terminal used by the target courier is the target courier terminal.

[0066] S409: sending, by the target courier terminal, an order verification request to the decentralized identity system, the order verification request including the order information.

[0067] It may be understood that the order verification request is generated by the target courier terminal based on the order information.

[0068] Exemplarily, the courier carries the terminal device (that is, the target courier terminal) to provide a shipping service for the user. When the courier arrives at an agreed pickup location

with the user, in order to perform verification on the user (that is, to perform the order verification), the courier clicks a verification control displayed on the terminal device, so as to enable the target courier terminal to send the order verification request to the decentralized identity system.

[0069] S410: performing, by the decentralized identity system, verification on the order information to obtain an order verification result.

[0070] In some embodiments, the order information received by the logistics management platform is order information that has been electronically signed by the user terminal using a private key. The performing, by the decentralized identity system, the verification on the order information to obtain the order verification result may include following steps: determining, by the decentralized identity system, a target public key based on the first DID in the order verification request, the target public key being a public key stored in the decentralized identity system that corresponds to the first DID; and performing, by the decentralized identity system, signature verification on the order information utilizing the target public key to obtain the order verification result. The method of using private key signing and public key signature verification to verify the order information is simple and easy to implement.

[0071] S411: sending, by the decentralized identity system, the order verification result to the target courier terminal.

[0072] The logistics management platform and the decentralized identity system performs the login verification on the user by utilizing the first DID and the first VC document filled in the user terminal by the user, and a login verification result is the identity verification result. By integrating the login verification and the identity verification into a single process, a verification procedure is simplified, and the method is simple and efficiency of the identity verification is relatively high. Moreover, since the identity verification is completed during a login process, no further identity verification is required in subsequent processes. That is, in a subsequent order placement process on the user terminal, only the order information needs to be verified, which enhances verification efficiency and improves processing efficiency of logistics order.

[0073] In some embodiments, when the order verification or the identity verification is performed by the decentralized identity system, the identity authentication server may be used for verification, or the blockchain may be used for smart contract verification.

[0074] The following provides an exemplary illustration of verification of the identity authentication server and the smart contract verification of the blockchain, taking the order verification as an example.

[0075] When the identity authentication server is utilized for verification, the identity authentication server determines the target public key corresponding to the user based on the first DID in the order verification request, and utilizes the target public key to perform signature verification on the order information to obtain the order verification result.

[0076] When the blockchain is utilized for smart contract verification, the target courier terminal determines a blockchain contract interface based on the first DID in the order verification request, thereby enabling the blockchain to complete the order verification. Performing the order verification by the blockchain may include following steps: determining, by the blockchain, the target public key corresponding to the user based on the first DID in the order verification request, and utilizing, by the blockchain, the target public key to perform signature verification on the order information to obtain the order verification result.

[0077] It should be understood that private key signing and public key signature verification are technical content easily understood by those skilled in the art, the details are not described in the embodiments of the present application again.

[0078] The following provides an exemplary illustration of verification of the identity authentication server and the smart contract verification of the blockchain, taking the process of performing the identity verification on the user based on the identity verification request as an example.

[0079] In some embodiments, when the identity authentication server is utilized for verification, the identity authentication server determines the target VC document stored in the identity authentication server that corresponds to the first DID based on the first DID in the identity verification request, and compares the determined target VC document with the first VC document to obtain the identity verification result.

[0080] It may be understood that when the determined target VC document is compared with the first VC document, if the target VC document is the same as the first VC document, the identity verification result is determined to be successful; and if the target VC document is different from the first VC document, the identity verification result is determined to be a failure.

[0081] In some other embodiments, when the identity authentication server is utilized for verification, the identity authentication server performs the signature verification on the first VC document by using the first public key to obtain the identity verification result. The first public key is a public key of the identity authentication server.

[0082] It may be understood that when the second VC document is generated by the identity authentication server for the user, the identity authentication server performs electronic

signature on the second VC document using its own private key. Therefore, during the identity verification, the identity authentication server performs the signature verification on the first VC document using its own first public key. If the signature verification is successful, it indicates that the first VC document is issued by the identity authentication server, and therefore, the identity verification result is determined to be successful; and if the signature verification fails, it indicates that the first VC document is not issued by the identity authentication server, and therefore, the identity verification result is determined to be a failure.

[0083] In some embodiments, when the blockchain is utilized for smart contract verification, the target courier terminal determines a blockchain contract interface based on the first DID in the identity verification request, thereby enabling the blockchain to complete the identity verification. Performing the identity verification by the blockchain may include following steps: determining, by the blockchain, the target VC document stored in the blockchain that corresponds to the first DID based on the first DID; and comparing, by the blockchain, the target VC document with the first VC document to obtain the identity verification result. It may be understood that if the target VC document is the same as the first VC document, the identity verification result is determined to be successful; and if the target VC document is different from the first VC document, the identity verification result is determined to be a failure.

[0084] In some other embodiments, the blockchain determines a public key of the identity authentication server based on identification information of the identity authentication server in the first VC document, and utilizes the public key of the identity authentication server to perform signature verification on the first VC document to obtain the identity verification result. When the identity verification result is determined by adopting public key signature verification, if the signature verification is successful, the identity verification result is determined to be successful; and if the signature verification fails, the identity verification result is determined to be a failure.

[0085] In some embodiments, after the order verification result is received by the target courier terminal, if the order verification result is determined to be successful, the target courier terminal prompts the courier that the verification is successful, and sends waybill generation instruction information to the logistics management platform, and then the logistics management platform generates a waybill based on the order information according to the waybill generation instruction information; and if the order verification result is determined to be a failure, the target courier terminal sends a request for terminating order placement to the logistics management platform, and then the logistics management platform sends an order placement failure reminder to the user terminal. In a case of successful verification, the logistics

management platform generates the waybill based on the order information, that is, the user successfully places an order. The method is simple and easy to implement. In a case that the verification fails, the logistics management platform sends an order placement failure reminder to the user terminal, thereby improving user experience.

[0086] In some embodiments, the login request includes a username and a password registered by the user terminal on the logistics management platform. It should be understood that since the user does not need to undergo the real-name authentication on the logistics management platform, the login verification based on the username and the password cannot realize the identity verification for the user. Since the logistics management platform does not perform the identity verification on the user during user login the logistics management platform, the identity verification may be performed before verification of the order information. An exemplary illustration of the identity verification method in this scenario will be provided below with reference to FIG. 5.

[0087] FIG. 5 is a schematic interaction diagram of an identity verification method provided by another embodiment of the present application. As shown in FIG. 5, the method may include steps S501 to S510. The following is a detailed explanation of each step with reference to FIG. 5.

[0088] S501: receiving, by the logistics management platform, a login request sent by the user terminal, the login request including a username and a password registered by the user on the logistics management platform.

[0089] S502: performing, by the logistics management platform, login verification on the user based on the login request.

[0090] S503: in a case of successful login, receiving, by the logistics management platform, a first DID, a first VC document, and order information sent by the user terminal.

[0091] S504: determining, by the logistics management platform, a target courier terminal from the plurality of courier terminals based on the order information.

[0092] S505: sending, by the logistics management platform, the first DID, the first VC document, and the order information to the target courier terminal.

[0093] It should be understood that transmission of the first DID and the first VC document may also be performed separately from transmission of the order information, which is not limited in the embodiments of the present application.

[0094] S506: generating, by the target courier terminal, an identity verification request based on the first DID and the first VC document.

[0095] S507: sending, by the target courier terminal, the identity verification request to the decentralized identity system.

[0096] S508: performing, by the decentralized identity system, identity verification on the user based on the identity verification request to obtain an identity verification result.

[0097] It should be understood that a process of performing the identity verification on the user by the decentralized identity system based on the identity verification request is basically the same as a process of performing the identity verification on the user by the decentralized identity system based on the identity verification request in the embodiments shown in FIG. 4. Details are not described herein again.

[0098] S509: in a case that the identity verification result is successfully verified, performing, by the decentralized identity system, verification on the order information to obtain an order verification result.

[0099] S510: sending, by the decentralized identity system, the order verification result to the target courier terminal.

[0100] The user may log in to the logistics management platform using the username and the password registered on the logistics management platform, and therefore, the login process is user-friendly. Moreover, before verification of the order information, the decentralized identity system performs the identity verification on the user based on the first DID and the first VC document sent by the user terminal. Only if the identity verification is successful will the verification of the order information proceed. In a case that the identity verification fails, there is no need to perform the order verification. Therefore, data processing load of the decentralized identity system may be reduced. The identity verification may confirm that the user using the user terminal is a real user (that is, the user and the real person are in a one-to-one correspondence), and the verification of the order information may confirm legality of an order, that is, the order is indeed placed by the user and has legal attributes.

[0101] In some embodiments, the target courier terminal uploads the first DID, the first VC document, the order information, and the waybill to the blockchain for storage. The waybill and data used for generating the waybill are stored on the blockchain, which may serve as evidence preservation. When the user questions the order, the waybill and the data used for generating the waybill may be served as evidence, which may prevent the user from later denying the generated waybill, thereby ensuring interests of the target courier terminal (or legitimate rights and interests of the courier).

[0102] It should be understood that the sequence numbers of the steps in the above embodiments do not imply an order of execution. An execution order of each process should

be determined by its function and internal logic, and should not impose any limitation on an implementation process of the embodiments of the present application.

[0103] An embodiment of the present application also provides a computer device 600. The computer device may be at least one of a user terminal, a courier terminal, a logistics management platform, and a decentralized identity system. As shown in FIG. 6, the computer device 600 includes: a processor 601, a memory 602, and a computer program 604 stored in the memory 602 and running on the processor 601. The computer program 604 may be run by the processor 601 to generate an instruction 603, and the processor 601 implements the methods described in the above embodiments based on the instruction 603.

[0104] Exemplarily, the computer program 604 may be divided into one or more modules/units, which are stored in the memory 602 and executed by the processor 601 to complete the methods described in the above embodiments. The one or more modules/units may be a series of computer program instruction segments capable of completing specific functions, which are used for describing an execution process of the computer program 604 in the computer device 600.

[0105] Those skilled in the art may understand that FIG. 6 is only an example of the computer device 600 and does not impose any restrictions on the computer device 600. The computer device 600 may include more or fewer components than shown in the figure, or may combine certain components or different components. For example, the computer device 600 may also include an input/output device, a network access device, a bus, or the like.

[0106] The processor 601 may be a Central Processing Unit (CPU), or other general-purpose processors, a Digital Signal Processor (DSP), an Application Specific Integrated Circuit (ASIC), a Field-Programmable Gate Array (FPGA), or other programmable logic devices, a discrete gate or a transistor logic device, a discrete hardware component, and so on. The general-purpose processor may be a micro-processor or the processor may be any conventional processor, and so on.

[0107] The memory 602 may be an internal storage unit of the computer device 600, such as a hard disk or a memory of the computer device 600. The memory 602 may also be an external storage device of the computer device 600, such as a plug-in hard disk equipped on the computer device 600, a Smart Media Card (SMC), a Secure Digital (SD) card, and a Flash Card. Further, the memory 602 may also include both the internal storage unit of the computer device 600 and the external storage device of the computer device 600. The memory 602 is configured to store computer programs as well as other programs and data required by the

computer device 600. The memory 602 may also be configured to temporarily store data that has been output or is about to output.

[0108] The embodiments of the present application also provide a logistics management platform, where the logistics management platform is configured to execute the steps performed by the logistics management platform in the identity verification method provided by any embodiment of the present application.

[0109] The embodiments of the present application also provide a decentralized identity system, where the decentralized identity system is configured to execute the steps performed by the decentralized identity system in the identity verification method provided by any embodiment of the present application.

[0110] With reference to FIG. 7, the embodiments of the present application also provide a computer-readable storage medium 700, where the computer-readable storage medium 700 stores a computer program or an instruction 710. When a computer reads and executes the computer program or the instruction 710, the computer is caused to execute the above methods described in various method embodiments.

[0111] The embodiments of the present application provide a computer program product. When the computer program product runs on a server, the server is caused to implement the identity verification method provided by any embodiment of the present application.

[0112] The embodiments of the present application also provide a chip, and the chip includes: a processing unit and a communication unit. The processing unit may be, for example, a processor, and the communication unit may be, for example, an input/output interface, a pin, or a circuit. The processing unit is configured to invoke and run a computer program or a computer instruction, so that a computer device equipped with the chip executes the identity verification method provided by any embodiment of the present application.

[0113] Optionally, the computer program or the computer instruction is stored in a storage unit.

[0114] Optionally, the storage unit is a storage unit within the chip, such as a register or cache. The storage unit may also be a storage unit located outside the chip, such as a ROM or other types of static storage devices that may store static information and instructions, such as a RAM. The processor mentioned above in any instance may be a CPU, a micro-processor, an ASIC, or one or more integrated circuits. The processing unit and the storage unit may be decoupled and set on different physical devices, and are connected by wired or wireless means, to achieve their respective functions, thereby supporting the chip to implement various functions

described in the above embodiments. Alternatively, the processing unit and the memory may also be coupled on a same device.

[0115] It may be understood that the chip provided by the embodiments of the present application may be an integrated circuit used for implementing the identity verification method described above. A main function of the chip is to execute the steps or processes defined by the identity verification methods in the embodiments of the present application, that is, to implement the identity verification methods in the embodiments of the present application through a hardware. The above-mentioned embodiments are only used to illustrate technical solutions of the present application and are not intended to limit it.

[0116] Although the present application has been described in detail with reference to foregoing embodiments, those skilled in the art should understand that they may still modify the technical solutions described in the foregoing embodiments or equivalently replace some of technical features. However, these modifications or replacements do not cause the essence of corresponding technical solutions to deviate from the spirit and scope of the technical solutions of the embodiments of the present application, and should be included within the protection scope of the present application.

CLAIMS

What is claimed is:

1. An identity verification method, applied to an identity verification system, wherein the identity verification system comprises a logistics management platform, a plurality of courier terminals, and a decentralized identity system, and the method comprises:

sending, by the logistics management platform or a target courier terminal, an identity verification request to the decentralized identity system, wherein the identity verification request comprises a first decentralized identifier DID and a first verifiable claim VC document, and the target courier terminal is one of the plurality of courier terminals;

performing, by the decentralized identity system, identity verification on a user based on the identity verification request to obtain an identity verification result; and

in a case that the identity verification result is successfully verified, performing, by the decentralized identity system, verification on order information to obtain an order verification result, and sending, by the decentralized identity system, the order verification result to the target courier terminal.

2. The method according to claim 1, further comprising:

receiving, by the logistics management platform, a login request sent by a user terminal, wherein the login request comprises the first DID and the first VC document;

generating, by the logistics management platform, the identity verification request based on the first DID and the first VC document; and

in a case of successful identity verification, sending, by the decentralized identity system, successful login information to the logistics management platform.

3. The method according to claim 2, further comprising:

in a case of successful login, receiving, by the logistics management platform, the order information sent by the user terminal;

determining, by the logistics management platform, the target courier terminal from the plurality of courier terminals based on the order information, and sending, by the logistics management platform, the order information to the target courier terminal; and

sending, by the target courier terminal, an order verification request to the decentralized identity system, wherein the order verification request comprises the order information.

4. The method according to claim 1, further comprising:

receiving, by the logistics management platform, a login request sent by a user terminal, and performing, by the logistics management platform, login verification on the user based on the login request, wherein the login request comprises a username and a password registered by the user on the logistics management platform;

in a case of successful login, receiving, by the logistics management platform, the first DID, the first VC document, and the order information sent by the user terminal, and determining, by the logistics management platform, the target courier terminal from the plurality of courier terminals based on the order information;

sending, by the logistics management platform, the first DID, the first VC document, and the order information to the target courier terminal;

generating, by the target courier terminal, the identity verification request based on the first DID and the first VC document; and

sending, by the target courier terminal, the order information to the decentralized identity system.

5. The method according to any one of claims 1 to 4, wherein the performing, by the decentralized identity system, the identity verification on the user based on the identity verification request to obtain the identity verification result comprises:

determining, by the decentralized identity system, a target VC document corresponding to the first DID based on the first DID, and comparing, by the decentralized identity system, the target VC document with the first VC document to obtain the identity verification result,

or, performing, by the decentralized identity system, signature verification on the first VC document using a first public key to obtain the identity verification result, wherein the first VC document is obtained by the decentralized identity system performing electronic signature using a private key of the decentralized identity system, and the first public key is a public key of the decentralized identity system.

6. The method according to any one of claims 1 to 5, wherein the order information is obtained by the user terminal performing electronic signature using a first private key, and the first private key is a private key stored in the user terminal that corresponds to the user; and

the performing, by the decentralized identity system, the verification on the order information to obtain the order verification result comprises:

determining, by the decentralized identity system, a target public key based on the first

DID, wherein the target public key is a public key stored in the decentralized identity system that corresponds to the first DID; and

performing, by the decentralized identity system, signature verification on the order information by using the target public key to obtain the order verification result.

7. The method according to any one of claims 1 to 6, wherein the decentralized identity system comprises an identity authentication server, a certification authority CA server, and a blockchain, and the method further comprises:

receiving, by the identity authentication server, a real-name registration request sent by the user terminal, wherein the real-name registration request comprises identity information of the user;

generating, by the identity authentication server, a second DID and a second VC document that correspond to the user based on the real-name registration request, and sending, by the identity authentication server, a key request to the CA server;

generating, by the CA server, a second public key and a second private key that correspond to the user based on the key request, and sending, by the CA server, the second public key and the second private key to the identity authentication service;

sending, by the identity authentication server, the second private key, the second DID, and the second VC document to the user terminal; and

storing, by the identity authentication server, the second public key, the second DID, and the second VC document.

8. The method according to any one of claims 1 to 7, wherein the decentralized identity system comprises an identity authentication server, a certification authority CA server, and a blockchain, and the method further comprises:

receiving, by the identity authentication server, a real-name registration request sent by the user terminal, wherein the real-name registration request comprises identity information of the user;

generating, by the identity authentication server, a second DID and a second VC document that correspond to the user based on the real-name registration request, and sending, by the identity authentication server, a key request to the CA server;

generating, by the CA server, a second public key and a second private key that correspond to the user based on the key request, and sending, by the CA server, the second public key and the second private key to the identity authentication service;

sending, by the identity authentication server, the second private key, the second DID, and the second VC document to the user terminal; and

uploading, by the identity authentication server, the second public key, the second DID, and the second VC document to the blockchain.

9. The method according to claim 7 or 8, wherein the performing, by the decentralized identity system, the identity verification on the user based on the identity verification request comprises:

performing, by the identity authentication server or the blockchain, the identity verification on the user based on the identity verification request.

10. The method according to any one of claims 7 to 9, wherein the performing, by the decentralized identity system, the verification on the order information comprises:

performing, by the identity authentication server or the blockchain, the verification on the order information.

11. The method according to any one of claims 1 to 10, further comprising:

if the order verification result is successfully verified, sending, by the target courier terminal, waybill generation instruction information to the logistics management platform; and

generating, by the logistics management platform, a waybill based on the order information according to the waybill generation instruction information.

12. The method according to claim 11, further comprising:

uploading, by the target courier terminal, the first DID, the first VC document, the order information, and the waybill to the blockchain for storage.

13. An identity verification system, comprising a logistics management platform, a plurality of courier terminals, and a decentralized identity system, the logistics management platform is configured to execute steps executed by the logistics management platform in the method according to any one of claims 1 to 12, one of the plurality of courier terminals is configured to execute steps executed by the target courier terminal in the method according to any one of claims 1 to 12, and the decentralized identity system is configured to execute steps executed by the decentralized identity system in the method according to any one of claims 1 to 12.

14. A computer-readable storage medium, wherein the computer-readable storage medium stores a computer program or an instruction, when a computer reads and executes the computer program or the instruction, the computer is caused to execute the method according to any one of claims 1 to 12.

15. A chip, comprising a processor configured to invoke and run a computer program from a memory, causing a computer device equipped with the chip to execute the method according to any one of claims 1 to 12.