TITLE OF INVENTION: DATA READ AUTHORITY CONTROL SYSTEM BASED ON BLOCK CHAIN AND ZERO-KNOWLEDGE PROOF MECHANISM, AND RELATED DATA SERVICE SYSTEM

BACKGROUND

[0001] The disclosure generally relates to a data read authority control technology and, more particularly, to a data read authority control system based on block chain and zero-knowledge proof mechanism, and a related data service system.

[0002] The General Data Protection Regulation (GDPR) formulated by the European Union is not only strict in its regulations for personal data and privacy protection, but also covers a wide range of scopes. If the GDPR cannot be met, commercial activity in many fields will face very significant impacts or obstacles.

[0003] Since the traditional OAuth 2.0 data authorization framework cannot meet various requirements of GDPR, various more complex data read authority control architectures are developed in response to the GDPR requirements. Various newly developed data read authority control architectures, including UMA 2.0 (User-Managed Access 2.0), use a centralized authorization server to manage the data read authority of individual data owners. Such structure may seem to meet the requirements of the GDPR, but in fact it is not transparent in the management of the data read authority, and it is also difficult to prove the authenticity of the data owner's relevant sensitive data to the data recipient (or other third party). Therefore, the existing data read authority control architectures are not very ideal solutions for many commercial applications (e.g., carbon rights transaction, various loan-gap lending services, reservation and payment for electric vehicle charging services, or the like).

SUMMARY

[0004] In view of the foregoing, it can be appreciated that a substantial need exists for a data read authority control system that not only meets various GDPR requirements of the EU, but can also effectively verify the authenticity of the data owner’s relevant sensitive data.

[0005] An example embodiment of a data read authority control system is disclosed, comprising: a block chain system; a data owner device arranged to operably receive data inputted by a target user to generate a target data, and to operably utilize a proof key to generate a proof; a data source system arranged to operably store a sensitive data corresponding to the target data; a data service system arranged to operably receive the target data and the proof

generated by the data owner device, and to operably request the block chain system to verify the proof; a data requester device arranged to operably generate and transmit a sensitive data request corresponding to the target data to the data service system; wherein the block chain system arranged to operably execute a zero-knowledge proof smart contract to utilize a verification key to verify correctness of the proof, and to operably transmit a verification success notification to the data service system when the proof is determined as correct; wherein the block chain system is further arranged to operably verify an activity of an authorization token corresponding to an authorization token identification data, and to operably generate and transfer a read token to the data service system when determining the authorization token as active; wherein the data service system is further arranged to operably transmit the sensitive data request to the data source system and transfer the read token to the data source system after acquiring the read token; wherein if the read token transferred from the data service system to the data source system is active, the data source system operably transmits the sensitive data corresponding to the target data to the data service system, and the data service system operably transmits the sensitive data to the data requester device.

[0006] An example embodiment of a data service system of a data read authority control system is disclosed, wherein the data read authority control system comprises a data owner device, a data requester device, a data source system, and a block chain system. The data service system comprises: a communication circuit arranged to operably receive a target data and a proof transmitted from the data owner device, and to operably receive a sensitive data request corresponding to the target data transmitted from the data requester device; a block chain computing circuit arranged to operably act as one node of the block chain system, and arranged to operably request the block chain system to verify the proof, wherein the block chain system executes a zero-knowledge proof smart contract to utilize a verification key to verify correctness of the proof; a database arranged to operably store the target data and a web server, coupled with the communication circuit, the block chain computing circuit, and the database, and arranged to operably acquire a read token transferred from the block chain system through the communication circuit or the block chain computing circuit when the block chain system determines an authorization token corresponding to an authorization token identification data as active; wherein the communication circuit is further arranged to operably receive a verification success notification transmitted from the block chain system when the proof is determined as correct by the block chain system; wherein the web server is further arranged to operably transmit the sensitive data request to the data source system through the communication circuit after acquiring the read token, and to operably transfer the read token

to the data source system through the communication circuit or the block chain computing circuit; wherein if the read token transferred from the data service system to the data source system is valid, the web server operably receives a sensitive data corresponding to the target data transmitted from the data source system through the communication circuit, and operably transmits the sensitive data to the data requester device to the communication circuit.

[0007] Both the foregoing general description and the following detailed description are examples and explanatory only, and are not restrictive of the invention as claimed.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] FIG. 1 shows a simplified functional block diagram of a data read authority control system according to one embodiment of the present disclosure.

[0009] FIG. 2 through FIG. 6 collectively show a simplified flowchart of a data read authority control method according to one embodiment of the present disclosure.

DETAILED DESCRIPTION

[0010] Reference is made in detail to embodiments of the invention, which are illustrated in the accompanying drawings. The same reference numbers may be used throughout the drawings to refer to the same or like parts, components, or operations.

[0011] FIG. 1 shows a simplified functional block diagram of a data read authority control system 100 according to one embodiment of the present disclosure. The data read authority control system 100 can be utilized for controlling the read authority of relevant data of various types of data owners such as individuals or enterprises, and can utilize a zero-knowledge proof (ZKP) mechanism to verify the authenticity of the data provided by the data owners.

[0012] The data read authority control system 100 comprises one or more data owner devices (e.g., the exemplary data owner devices 110~120 shown in FIG. 1), one or more data requester devices (e.g., the exemplary data requester devices 130 ~140 shown in FIG. 1), one or more data source system (e.g., the exemplary data source system 150 shown in FIG. 1), a data service system 160, a block chain node cluster 170, and a block chain system 180 collectively formed by the block chain node cluster 170 cooperating with other block chain computing circuits.

[0013] The multiple data owner devices 110~120 in the data read authority control system 100 respectively belong to different data owners, and each of the data owners may be an individual, an enterprise or company organization of various types, a foundation of various

types, a corporate legal person of various types, a non-profit organization of various types, a government institution of various types, or the like.

[0014] The multiple data requester devices 130~140 in the data read authority control system 100 respectively belong to different data owners, and each of the data owners may be an individual, an enterprise or company organization of various types, a foundation of various types, a corporate legal person of various types, a non-profit organization of various types, a government institution of various types, or the like.

[0015] The data source system 150 may be a system operated by a specific service provider of digital storage services (e.g., various online storage service providers, banks, financial institutions, credit card issuers, government units, etc.), and utilized to store various digital data provided by individual data owners or relevant to individual data owners, such as various digital files, various program files, and/or various multimedia data, or the like.

[0016] The data service system 160 may be a system operated by a specific service provider, e.g., various online trading platforms, online book rental platforms, online multimedia rental platforms, non-fungible token (NFT) trading platforms, or the like, that can provide various online transaction services, online loan matching services, online book rental services, online multimedia rental services, and/or NFT transaction services. The data service system 160 is arranged to operably manage the use authorities, data browsing authorities, transaction authorities, or the like of respective data owners and/or respective data requesters.

[0017] In addition, the block chain system 180 is usually a blockchain system jointly operated and managed by multiple different entities. The block chain system 180 is utilized to control the data read authorities of the data stored in the data source system 150, and allows individual data owners to utilize corresponding data owner devices to dynamically adjust their data authorization policies.

[0018] In practical applications, the various digital data stored in the data source system 150 may be transmitted to the data source system 150 by individual data owners through related devices (e.g., the data owner devices), may be inputted to the data source system 150 by operators having authority, or may be generated by the data source system 150 when executing predetermined computer programs.

[0019] Each data owner may log in to the data service system 160 through the corresponding data owner device and create specific target data (e.g., specific documents, files, descriptive texts, contract terms, transaction conditions, or the like). Additionally, each data owner may further utilize the data owner device to transmit data authorization policies for different data requesters to the block chain system 180 for storage and management, so as to prevent data

authorization policies from being tampered with. The aforementioned data authorization policy may comprise part of or all of multiple parameters such as an authorized target, an authorized data subject, an authorization content, an upper limit of authorization times, an authorization period, an authorization time limit, a geographical area where the data is located, an identification data of the data source system 150 that stores the data (e.g., an address of a specific smart contract deployed by the data source system 150 in the block chain system 180), or the like.

[0020] After receiving the target data transmitted from the data owner device, the data service system 160 may operate with the block chain system 180 to verify the authenticity of all or part of the target data. In operations, the block chain system 180 may execute specific smart contracts to adopt a ZKP verification mechanism to verity the authenticity of a proof generated by the data owner device, so as to indirectly verify the authenticity of all or part of the target data. In practice, the block chain system 180 may execute specific smart contracts deployed by the data source system 150 to conduct related ZKP verification operation.

[0021] On the other hand, an individual data requester may control the corresponding data requester device to request the data service system 160 for providing specific data corresponding to a specific data owner. In this situation, the data service system 160 may request the block chain system 180 for providing a data read token corresponding to specific data, and the block chain system 180 may execute specific smart contracts to determine whether the data service system 160 should provide data read token to the data service system 160.

[0022] After acquiring the data read token generated by the block chain system 180, the data service system 160 may transmit a related data request to the data source system 150 and transfer the data read token to the data source system 150. In this situation, the data source system 150 may utilize the block chain system 180 to verify the activity of the data read token. The data source system 150 provides specific data contents corresponding to the specific data owner to the data service system 160 only if the activity of the data read token passes the verification of the block chain system 180, so that the data service system 160 can provide the specific data contents to the data requester device.

[0023] In addition, the block chain system 180 may record related temporal data of respective data read tokens to be the supporting evidence for proving that the data service system 160 retrieve specific data contents.

[0024] In the data read authority control system 100, each data owner may further dynamically adjust the data authorization policy stored in the block chain system 180 as needed. For example, after a data owner adjusts the data authorization policy for the data service system

160, specific data requesters, or all data requesters due to various reasons, the data owner may utilize the related data owner device to transmit updated data authorization policy to the block chain system 180 for storage and management, so as to replace the data authorization policy of the former version.

[0025] In order to meet the needs of some commercial transactions or legal relationship management, different participants in the data read authority control system 100 may adopt traditional approaches or digital approaches to sign various appropriate agreements or contracts to further clarify the legal relationship between each other. For example, each data owner and a specific service provider operating the data source system 150 may jointly sign various appropriate transaction agreements, loan agreements, investment agreements, data hosting agreements, online storage space lease contracts, service agreements, intellectual property ownership agreements, data transmission agreements, privacy protection agreements, data sharing agreements, and/or personalized advertising broadcast agreements, or the like.

[0026] For another example, each data owner and a specific service provider operating the data service system 160 may jointly sign various appropriate transaction matching agreements, investment target matching agreements, loan matching agreements, data licensing agreements, data sharing agreements, data utilization agreements, data inspection agreements, and/or data auditing agreements, or the like.

[0027] For yet another example, each data owner and a specific service provider operating the block chain system 180 may jointly sign various appropriate block chain service agreements.

[0028] For yet another example, each data owner and each data requester may jointly sign various appropriate transaction agreements, investment agreements, loan agreements, data authorization agreements, data sharing agreements, data utilization agreements, data inspection agreements, and/or data audit agreements, or the like.

[0029] For another example, each data requester and a specific service provider operating the data service system 160 may jointly sign various appropriate transaction matching agreements, investment target matching agreements, loan matching agreements, data index generation agreements, data query agreements, data sharing agreements, data utilization agreements, data transmission agreements, and/or service agreements, or the like.

[0030] As shown in FIG. 1, the data owner device 110 comprises a communication circuit 111, a block chain computing circuit 113, a display device 115, and a control circuit 117. The data requester device 130 comprises a communication circuit 131, a display device 133, and a control circuit 135. The data source system 150 comprises a communication circuit 151, a block chain computing circuit 153, a database 155, and a data server 157. The data service

system 160 comprises a communication circuit 161, a block chain computing circuit 163, a database 165, and a web server 167. The block chain node cluster 170 comprises multiple block chain nodes, such as the exemplary block chain nodes 171~177 shown in FIG. 1.

[0031] In the data owner device 110, the communication circuit 111 is arranged to operably conduct data communications with the data source system 150, the data service system 160, and/or the block chain system 180 through the Internet or other networks. The block chain computing circuit 113 is coupled with the communication circuit 111, and utilized to act as one of the nodes of the block chain system 180, and may serve as a communication bridge between the data owner device 110 and the block chain system 180. The display device 115 is arranged to operably display texts, data, and/or images. The control circuit 117 is coupled with the communication circuit 111, the block chain computing circuit 113, and the display device 115, and arranged to operably control operations of the aforementioned devices.

[0032] In the data requester device 130, the communication circuit 131 is arranged to operably conduct data communications with the data service system 160 through the Internet or other networks. The display device 133 is coupled with the communication circuit 131, and arranged to operably display texts, data, and/or images. The control circuit 135 is coupled with the communication circuit 131 and the display device 133, and arranged to operably control operations of the aforementioned devices.

[0033] Each of other data owner devices in the data read authority control system 100 (e.g., the data owner device 120) may have a similar main structure to that of the data owner device 110, but it does not require all of the data owner devices to have identical circuit structure with each other in practical implementations. Similarly, each of other data requester devices in the data read authority control system 100 (e.g., the data requester device 140) may have a similar main structure to that of the data requester device 130, but it does not require all of the data requester devices to have identical circuit structure with each other in practical implementations.

[0034] In the data source system 150, the communication circuit 151 is arranged to operably conduct data communications with the data service system 160, the block chain system 180, and/or respective data owner devices through the Internet or other networks. The block chain computing circuit 153 is coupled with the communication circuit 151, and utilized to act as one of the nodes of the block chain system 180, and may serve as a communication bridge between the data source system 150 and the block chain system 180. The database 155 is arranged to operably store data corresponding to different data owners. The data server 157 is coupled with the communication circuit 151, the block chain computing circuit 153, and the database

155, and arranged to operably control operations of the aforementioned devices.

[0035] In the data service system 160, the communication circuit 161 is arranged to operably conduct data communications with the data source system 150, the block chain system 180, respective data owner devices, and/or respective data requester devices. The block chain computing circuit 163 is coupled with the communication circuit 161, and utilized to act as one of the nodes of the block chain system 180, and may serve as a communication bridge between the data service system 160 and the block chain system 180. The database 165 is arranged to operably store various data required by data service system 160 for realizing various applications. The web server 167 is coupled with the communication circuit 161, the block chain computing circuit 163, and the database 165, and arranged to operably control operations of the aforementioned devices.

[0036] In practical applications, the aforementioned data source system 150 may be a system for providing a single type of service (e.g., online banking services, financial services, contract file management services, cloud storage services, multimedia file sharing services, life record sharing services, community services, financial management services, health information management services, or the like), or may be a system for providing multiple compound services, e.g., a cloud storage service with an email service, a multimedia data sharing service with an instant messaging service, a community service with a multimedia streaming service, an ERP (enterprise resource planning) cloud service with a database service, or the like.

[0037] The block chain system 180 in this embodiment is collectively formed by the block chain computing circuit 113 of the data owner device 110, the block chain computing circuit 153 of the data source system 150, the block chain computing circuit 163 of the data service system 160, and the multiple block chain nodes 171~177 of the block chain node cluster 170.

[0038] In practice, each of the communication circuits 111, 131, 151, and 161 may be realized with various suitable circuits complying with relevant network communication protocols, wireless communication protocols, or mobile communication protocols, such as a NIC (Network Interface Cards), a Wi-Fi circuit, a mobile communication circuit, or the like. Each of the block chain computing circuits 113, 153, 163, and the block chain nodes 171~177 may be realized with one or more processor modules or a computer system suitable for performing a consensus algorithm of the block chain. Each of the display devices 115 and 133 may be realized with various devices capable of displaying texts, data, graphs, and/or images, such as various screens, projectors, televisions, or the like. Each of the databases 155 and 165 may be realized with various relational databases, or non-relational databases. Each of the

control circuits 117 and 135 may be realized with one or more processor modules, a single computer system, or a combination of multiple computer systems having appropriate computing capability. Each of the data server 157 and the web server 167 may be realized with a single server, or may be realized with the combination of multiple servers located in the same geographical region or in different geographical regions.

[0039] In some embodiments, the block chain computing circuit 113 may be integrated into the control circuit 117. Similarly, the block chain computing circuit 153 may be integrated into the data server 157, and/or the block chain computing circuit 163 may be integrated into the web server 167.

[0040] Please note that each of the aforementioned data owner device 110, data requester device 130, and data source system 150, and data service system 160 may be equipped with other human interface devices (e.g., monitors, keyboards, computer mouses, touch screens, voice control modules, or the like) for the users to manipulate in the practical implementations. In order to simplify the complexity of the drawing, these human interface devices are not illustrated in FIG. 1.

[0041] In the application environment where the data owner corresponding to the data owner device 110 is an individual, the data owner device 110 may be realized with a terminal device having networking capabilities and appropriate computing capabilities, such as a tablet computer, a desktop computer, a notebook computer, a mobile communication device (e.g., a smart phone, a wearable device, or the like), or other similar devices. Similarly, in the application environment where the data requester corresponding to the data requester device 130 is an individual, the data requester device 130 may be realized with a terminal device having networking capabilities and appropriate computing capabilities, such as a tablet computer, a desktop computer, a notebook computer, a mobile communication device (e.g., a smart phone, a wearable device, or the like), or other similar devices.

[0042] In the application environment where the data owner corresponding to the data owner device 110 is an enterprise or company organization of various types, a foundation of various types, a corporate legal person of various types, a non-profit organization of various types, or a government institution of various types, the data owner device 110 may be realized with a terminal device or an information system having networking capabilities and appropriate computing capabilities, such as a tablet computer, a desktop computer, a notebook computer, a mobile communication device, a computer server, a MIS (management information system), an ERP system, or other similar equipments. Similarly, in the application environment where the data requester corresponding to the data requester device 130 is an enterprise or a company

organization of various types, a foundation of various types, a corporate legal person of various types, a non-profit organization of various types, or a government institution of various types, the data requester device 130 may be realized with a terminal device or an information system having networking capabilities and appropriate computing capabilities, such as a tablet computer, a desktop computer, a notebook computer, a mobile communication device, a computer server, a MIS, an ERP system, or other similar equipments.

[0043] For the convenience of description, a specific data owner corresponding to the data owner device 110 is hereinafter referred to as a data owner D1; a specific data owner corresponding to the data owner device 120 is hereinafter referred to as a data owner D2; a specific data requester corresponding to the data requester device 130 is hereinafter referred to as a data requester R1; and a specific data requester corresponding to the data requester device 140 is hereinafter referred to as a data requester R2.

[0044] In practice, each of the aforementioned data owner device 110, data requester device 130, data source system 150, and data service system 160 may be realized with a virtual machine installed on various cloud platforms, or a combination of various computing entities and storage entities, and may be remotely controlled by their respective users.

[0045] In addition, in some application environments, the block chain system 180 may be realized with various public chain architectures. In other application environments, the block chain system 180 may be realized with a private chain architecture or a consortium chain architecture to shorten the time required for related computations and to improve the operation efficiency of the block chain system 180.

[0046] The operations of controlling data read authority conducted by the data read authority control system 100 will be further described below by reference to FIG. 2 through FIG. 6. FIG. 2 through FIG. 6 show a simplified flowchart of a data read authority control method according to one embodiment of the present disclosure.

[0047] In the flowcharts of FIG. 2 through FIG. 6, operations within a column under the name of a specific device are operations to be performed by the specific device. For example, operations within a column under the label “data owner device” are operations to be performed by any one of the data owner devices 110~120; operations within a column under the label “data requester device” are operations to be performed by any one of the data requester devices 130 ~140; operations within a column under the label “data source system” are operations to be performed by the data source system 150; operations within a column under the label “data service system” are operations to be performed by the data service system 160; and operations within a column under the label “block chain system” are operations to be performed by the

block chain system 180.

[0048] As described previously, the data read authority control system 100 can be utilized for controlling the read authority of relevant data of various types of data owners such as individuals or enterprises, and can utilize a zero-knowledge proof (ZKP) mechanism to verify the authenticity of the data provided by the data owners. Accordingly, the data read authority control system 100 can be utilized to realize many applications of different scenarios. For example, the data read authority control system 100 may be utilized for assisting respective users to conduct various loan-gap lending activity.

[0049] As is well known in the art, many individuals or enterprises need to apply for loans (e.g., home loans/housing loans, land loans, car loans, credit loans, or the like) from financial institutions such as banks when purchasing houses, land, cars, aircraft, or other types of movable properties or real estates. However, due to various reasons (e.g., policy restrictions, credit rating restrictions, or insufficient collateral), the financial institutions such as banks may not be able to approve the loan applicant's loan amount in full, and thus the loan applicant will face a loan-gap issue.

[0050] In some loan scenarios, if the loan applicant is unable to raise funds on his own to fill the loan gap by the deadline required by the financial institution, it may even lead to that the loan application being rejected by the financial institution. However, filling a loan gap is not an easy task for many loan applicants, especially when there is time pressure. In this situation, the data read authority control system 100 can be utilized to assist the loan applicant to initiate a loan-gap lending to other individuals or investment units (e.g., the aforementioned data requesters), so as to assist the loan applicant to deal with the loan gap problem.

[0051] For ease of understanding, an application scenario where the data read authority control system 100 is utilized to assists a loan applicant to conduct a home-loan-gap lending/housing-loan-gap lending through the data service system 160 will be taken as an example to illustrate the data read authority control operation of the data read authority control system 100.

[0052] In general, when an individual loan applicant applies for a home loan/housing loan from a financial institution such as a bank, the financial institution such as the bank will assess the job nature, credit status, income status, debt repayment ability, and/or other conditions of the loan applicant to conduct credit investigations and generate corresponding credit evaluation reports. Additionally, the financial institution such as the bank will also investigate and appraise the condition and value of the relevant loan object (that is, the house to be purchased by the loan applicant in this example), and generate a corresponding assessment report.

[0053] After conducting various evaluation procedures, if the financial institution such as the bank finds that the loan application of the loan applicant is acceptable, the financial institution will generate and provide relevant loan contract documents (or loan contract draft documents) to the loan applicant. When the approved loan amount agreed by the financial institution is lower than the amount required by the loan applicant, a home loan gap/housing loan gap Y occurs. For example, the aforementioned home loan gap/housing loan gap Y may be the house price P minus the approved loan amount L (i.e., Y=P-L). For another example, the aforementioned home loan gap/housing loan gap Y may be the house price P minus both the down payment D prepared by the loan applicant and the approved loan amount L (i.e., Y=P-D-L). For yet another example, the aforementioned home loan gap/housing loan gap Y may be the house price P pluses the estimated decoration fee C and minus both the down payment D prepared by the loan applicant and the approved loan amount L (i.e., Y=P+C-D-L). Some financial institutions require the loan applicant to find a way to fill the home loan gap/housing loan gap within a specified period, otherwise the home loan/housing loan application will be rejected.

[0054] For the convenience of elaboration purpose, it is assumed hereinafter that the aforementioned loan applicant (or borrower party) is the data owner D1 corresponding to the data owner device 110 and that the aforementioned financial institution is the operating unit of the data source system 150. In addition, it is also assumed hereinafter that the investor (or lender party) that may lend money to the loan applicant is the data requester R1 corresponding to the aforementioned data requester device 130 and/or the data requester R2 corresponding to the aforementioned data requester device 140.

[0055] As described previously, when the data owner D1 applies for a home loan/housing loan to a financial institution (i.e., the operating unit of the data source system 150), the operating unit of the data source system 150 may generate a credit evaluation report corresponding to the data owner D1, and an assessment report corresponding to the loan object (i.e., the house to be purchased by the data owner D1). If the operating unit of the data source system 150 determines that the loan can be made to the data owner D1 after evaluation, a loan contract document/loan contract draft document corresponding to the data owner D1 may also be generated.

[0056] Similarly, when other loan applicants (e.g., the data owner D2 corresponding to the data owner device 120) apply for home loans/housing loans to the operating unit of the data source system 150, the operating unit of the data source system 150 may also generate related credit evaluation reports, assessment reports, and/or loan contract documents/loan contract

draft documents.

[0057] The aforementioned credit evaluation reports, assessment reports, and/or loan contract documents/loan contract draft documents related to individual loan applicants are, to some extent, sensitive data corresponding to individual loan applicants. Since the contents of these sensitive data involve the personal information or privacy of individual loan applicants, individual loan applicants can also be regarded as the owners of relevant sensitive data from a certain perspective.

[0058] As shown in FIG. 2, when the operating unit of the data source system 150 generates sensitive data (e.g., the aforementioned credit evaluation reports, assessment reports, and/or loan contract documents/loan contract draft documents) related to individual loan applicants, the data source system 150 may be utilized to perform the operation 202.

[0059] In the operation 202, the administrator or operator of the data server 157 may utilize the database 155 to store multiple sensitive data respectively corresponding to different data owners (e.g., different loan applicants). It can be appreciated from the foregoing descriptions that the sensitive data stored in the database 155 may be credit evaluation reports, assessment reports, and/or loan contract documents/loan contract draft documents relevant to respective loan applicants. In other words, the operation 202 may be performed intermittently. In normal situations, in order to ensure the rights and interests of loan applicants, the operating unit of the data source system 150 will not provide the aforementioned sensitive data related to loan applicants stored in the database 155 to third parties without obtaining the consent of the loan applicants.

[0060] In the operation 204, the data server 157 may establish a corresponding relationship between each data owner and a corresponding pair of proof key and verification key. For example, the data server 157 may establish a corresponding relationship between the data owner D1 and a corresponding pair of proof key PK1 and verification key VK1. Similarly, the data server 157 may establish a corresponding relationship between the data owner D2 and a corresponding pair of proof key PK2 and verification key VK2. In practice, the key pairs corresponding to different data owners are different.

[0061] As shown in FIG. 2, the administrator or operator of the data source system 150 may utilize the data source system 150 to operate with the block chain system 180 to perform the operation 206 through the operation 210, so as to deploy related smart contracts, which are required for the data service system 160 in verifying the proofs generated by respective data owner devices, in the block chain system 180.

[0062] In the operation 206, the data server 157 may establish one or more zero-knowledge

proof smart contracts SC-ZKP under the control of its manager or operator according to a pairing relationship between the proof key and the verification key of the individual data owner and a predetermined verification rule. The predetermined verification rule may comprise one or more constraints. In practice, the data server 157 may respectively establish multiple different zero-knowledge proof smart contracts SC-ZKP for different data owners, or may integrate the pairing relationship of key pairs corresponding to different data owners into a single zero-knowledge proof smart contract SC-ZKP.

[0063] In this embodiment, the data server 157 may incorporate the pairing relationship between the proof key PK1 and the verification key VK1 corresponding to the data owner D1 and a first predetermined verification rule into a dedicated zero-knowledge proof smart contract SC-ZKP. The first predetermined verification rule may comprise one or more constraints, whose correct information supposedly may only know by the data owner D1 and the operating unit of the data source system 150.

[0064] For example, the constraints of the first predetermined verification rule may require that a difference obtained by subtracting an approved loan amount from a house price should be equal to a predetermined loan gap amount.

[0065] For another example, the constraints of the first predetermined verification rule may require that a result of performing an appropriate hashing algorithm operation on a house price and a first random value should be identical to a first predetermined hash value, wherein the first random value is randomly selected by the data server 157, and the data owner D1 is not informed of the first random value.

[0066] For yet another example, the constraints of the first predetermined verification rule may require that a result of performing an appropriate hashing algorithm operation on an approved loan amount and a second random value should be identical to a second predetermined hash value, wherein the second random value is randomly selected by the data server 157, and the data owner D1 is not informed of the second random value.

[0067] For yet another example, the constraints of the first predetermined verification rule may require that a password to be verified should be identical to a unique password assigned to the data owner D1 by the operating unit of the data source system 150.

[0068] For yet another example, the constraints of the first predetermined verification rule may require that an identification data to be verified should be identical to a unique identification data corresponding to the data owner D1 (e.g., an ID number of the data owner D1, a value-added tax number of the data owner D1, or a document number of a loan document provided to the data owner D1 by the operating unit of the data source system 150).

[0069] For yet another example, the constraints of the first predetermined verification rule may require that a house price should be equal to a first predetermined amount.

[0070] For yet another example, the constraints of the first predetermined verification rule may require that an approved loan amount should be equal to a second predetermined amount.

[0071] In some embodiments, the first predetermined verification rule may comprise only one of the different constraints described above. In other embodiments, the first predetermined verification rule may comprise a plurality of constraints out of the different constraints described above.

[0072] Similarly, the data server 157 may incorporate the pairing relationship between the proof key PK2 and the verification key VK2 corresponding to the data owner D2 and a second predetermined verification rule into another different zero-knowledge proof smart contract SC-ZKP.

[0073] Alternatively, the data server 157 may incorporate the pairing relationship between the proof key PK1 and the verification key VK1 corresponding to the data owner D1, a first predetermined verification rule corresponding to the data owner D1, the pairing relationship between the proof key PK2 and the verification key VK2 corresponding to the data owner D2, and a second predetermined verification rule corresponding to the data owner D2 into a same zero-knowledge proof smart contract SC-ZKP in an appropriate form.

[0074] In the operation 208, the data server 157 may utilize the communication circuit 151 or the block chain computing circuit 153 to use a predetermined token corresponding to the data source system 150 to transmit the generated one or more zero-knowledge proof smart contracts SC-ZKP to the block chain system 180, and to instruct the block chain system 180 to authenticate the aforementioned zero-knowledge proof smart contract SC-ZKP.

[0075] In this situation, the block chain system 180 performs the operation 210 to utilize multiple nodes to perform an appropriate consensus algorithm to authenticate the received zero-knowledge proof smart contract SC-ZKP. If the zero-knowledge proof smart contract SC-ZKP passes the authentication of the block chain system 180, the block chain system 180 stores the aforementioned zero-knowledge proof smart contract SC-ZKP in the form of data blocks in the block chain ledger of the block chain system 180, so as to complete a procedure of deploying the aforementioned zero-knowledge proof smart contract SC-ZKP in the block chain system 180.

[0076] On the other hand, the operator of the block chain system 180 or specific personnel with authority may utilize an appropriate programming method to deploy related smart contracts required for subsequent data read authority control in the block chain system 180. In

practical applications, the aforementioned specific personnel with authority may be a specific person in an operation team collectively formed by the operating unit of the block chain system 180, the operating unit of the data source system 150, the operating unit of the data service system 160, relevant data owners, and/or relevant data requesters, or may be a specific person participated in the operation of the data read authority control system 100.

[0077] For example, the operator or the constructor of the block chain system 180 may edit and create a smart contract that comprises token management rules, and may utilize an appropriate communication device (e.g., a computer) to transmit the smart contract in the form of a transaction message to the block chain system 180, and to instruct the block chain system 180 to authenticate the smart contract.

[0078] In this situation, the block chain system 180 performs the operation 212 to utilize multiple nodes to perform an appropriate consensus algorithm to authenticate the smart contract comprising the token management rules. If the smart contract passes the authentication of the block chain system 180, the block chain system 180 stores the smart contract in the form of data blocks in the block chain ledger of the block chain system 180, so as to complete a procedure of deploying a token management smart contract SC-TM in the block chain system 180. In subsequent operations, the block chain system 180 may utilize the token management smart contract SC-TM to inspect and control the activity of different tokens corresponding to respective data owners.

[0079] Similarly, the operator or the constructor of the block chain system 180 may edit and create a smart contract that comprises data authorization policy management rules, and may utilize an appropriate communication device (e.g., a computer) to transmit the smart contract in the form of a transaction message to the block chain system 180, and to instruct the block chain system 180 to authenticate the smart contract.

[0080] In this situation, the block chain system 180 performs the operation 214 to utilize multiple nodes to perform an appropriate consensus algorithm to authenticate the smart contract comprising the data authorization policy management rules. If the smart contract passes the authentication of the block chain system 180, the block chain system 180 stores the smart contract in the form of data blocks in the block chain ledger of the block chain system 180, so as to complete a procedure of deploying an authorization policy smart contract SC-PL in the block chain system 180. In subsequent operations, the block chain system 180 may utilize the authorization policy smart contract SC-PL to conduct a version control over the data authorization policies configured by respective data owners.

[0081] In the operation 216, the data server 157 may transmit the proof key corresponding

to an individual target user to a corresponding data owner device through the communication circuit 151 or the block chain computing circuit 153. For example, the data server 157 may transmit the proof key PK1 corresponding to the data owner D1 to the corresponding data owner device 110 through the communication circuit 151 or the block chain computing circuit 153. In this situation, the data owner device 110 may perform the operation 218 to utilize the communication circuit 111 to receive the proof key PK1 provided by the data source system 150.

[0082] Similarly, the data server 157 may transmit the proof key PK2 corresponding to the data owner D2 to the corresponding data owner device 120 through the communication circuit 151 or the block chain computing circuit 153. In this situation, the data owner device 120 may perform the operation 218 to receive the proof key PK2 provided by the data source system 150.

[0083] In practice, the data source system 150 may transmit related proof keys to different data owner devices at the same time point, or may transmit related proof keys to different data owner devices at different time points.

[0084] In some embodiments, the data server 157 may also transmit the identification data of the verification key corresponding to the target user to the corresponding data owner device through the communication circuit 151 or the block chain computing circuit 153. For example, the data server 157 may transmit the identification data of the verification key VK1 corresponding to the data owner D1 to the corresponding data owner device 110 through the communication circuit 151 or the block chain computing circuit 153. In this situation, the data owner device 110 may utilize the communication circuit 111 to receive the identification data of the verification key VK1 provided by the data source system 150. Similarly, the data server 157 may transmit the identification data of the verification key VK2 corresponding to the data owner D2 to the corresponding data owner device 120 through the communication circuit 151 or the block chain computing circuit 153. In this situation, the data owner device 120 may receive the identification data of the verification key VK2 provided by the data source system 150.

[0085] In another embodiment, the data server 157 may transmit the identification data of the data owner devices corresponding to respective target users, the identification data of the verification keys corresponding to respective target users, and/or the identification data corresponding to respective target users to the data service system 160 and/or the block chain system 180 through the communication circuit 151 or the block chain computing circuit 153. In this situation, the communication circuit 161 of the data service system 160 and/or the block

chain system 180 may receive the above identification data provided by the data source system 150.

[0086] As described previously, the data read authority control system 100 is able to assist the data owner D1 to initiate a home-loan-gap lending/housing-loan-gap lending to other individuals or investment units through the data service system 160 to request other individuals or investment units to lend funds to the data owner D1. As long as other individuals or investment units agree to lend sufficient funds to the data owner D1, the data owner D1 can thus solve the home loan gap/housing loan gap problems with their assistance.

[0087] When the target user wants to utilize the data service system 160 to conduct a predetermined activity, the corresponding data owner device may perform the operation 220 of FIG. 2 to request the target user to input some data of relatively low-sensitivity and one or more data to be verified to be relevant data of the predetermined activity.

[0088] In this embodiment, for example, when the data owner D1 wants to utilize the data service system 160 to conduct a home-loan-gap/housing-loan-gap lending activity, the data owner D1 may manipulate the data owner device 110 to log in to the data service system 160 to create a home-loan-gap/housing-loan-gap lending case, thereby initiating a home-loan-gap/housing-loan-gap lending activity. In this situation, the web server 167 of the data service system 160 may generate and transmit relevant data filling pages to the data owner device 110, and the communication circuit 111 of the data owner device 110 may receive the data filling pages transmitted from the web server 167.

[0089] In this situation, the control circuit 117 may perform the operation 220 to control the display device 115 to display the data filling pages provided by the web server 167, so as to request the target user (e.g., the data owner D1 in this embodiment) to input some data of relatively low-sensitivity and one or more data to be verified.

[0090] The aforementioned data of relatively low-sensitivity may comprise the user's nickname, total borrowing amount, the borrowing period, the borrowing interest rate, the interest payment period, the principal amortization period, and/or other general information that does not involve the personal privacy of the data owner D1. In some embodiments, the aforementioned data of relatively low-sensitivity may comprise some basic information of the loan object (e.g., geographic area, age, floor, or the like of the house to be purchased by the data owner D1 in this example).

[0091] In one embodiment, the aforementioned data to be verified is a house price. In another embodiment, the aforementioned data to be verified is an approved loan amount. In yet another embodiment, the aforementioned data to be verified are a house price and an

approved loan amount. In yet another embodiment, the aforementioned data to be verified is a unique password assigned to the data owner D1 by the operating unit of the data source system 150. In yet another embodiment, the aforementioned data to be verified is a unique identification data corresponding to the data owner D1 (e.g., an ID number of the data owner D1, a value-added tax number of the data owner D1, or a document number of a loan document provided to the data owner D1 by the operating unit of the data source system 150).

[0092] In some embodiments, the data to be verified that the display device 115 requires the data owner D1 to input may comprise only one of the different data items described above. In other embodiments, the data to be verified that the display device 115 requires the data owner D1 to input may comprise a plurality of data items out of the different data items described above.

[0093] In practical applications, the data owner D1 may input the aforementioned data of relatively low-sensitivity and the data to be verified to the data owner device 110 through various appropriate input interfaces (not shown in the drawings). In this situation, the control circuit 117 of the data owner device 110 may perform the operation 222 to receive the data of relatively low-sensitivity and the data to be verified inputted by the target user (e.g., the data owner D1 in this embodiment) through the corresponding input interfaces.

[0094] In the operation 224, the control circuit 117 may generate a corresponding target data according to the received data of relatively low-sensitivity. In operations, the control circuit 117 may organize and/or encode the received data of relatively low-sensitivity into a suitable format, so as to generate a corresponding target data as the description data for the home-loan-gap/housing-loan-gap lending case initiated by the data owner D1.

[0095] In some embodiments, the data filling pages provided by the web server 167 may additionally request the data owner D1 to input some data of relatively high-sensitivity related to the personal information of the data owner D1, such as name, occupation, age, gender, income level, marital status, number of children, and/or credit rating, or the like.

[0096] In this situation, the data owner D1 may input the aforementioned data of relatively low-sensitivity, data to be verified, and data of relatively high-sensitivity to the data owner device 110 through various appropriate input interfaces. In this embodiment, the control circuit 117 may further receive the data of relatively high-sensitivity inputted by the data owner D1 through various appropriate input interfaces in the operation 222. In addition, the control circuit 117 may also incorporate the aforementioned data of relatively high-sensitivity into the target data in the operation 224.

[0097] It can be appreciated from the foregoing descriptions that the target data generated

by the control circuit 117 in the operation 224 may merely comprise the data of relatively low-sensitivity of the data owner D1, or may further comprise the data of relatively high-sensitivity corresponding to the data owner D1.

[0098] In the operation 226, the control circuit 117 may utilize the proof key PK1 to generate a proof PF1 according to the received data to be verified. In practice, the control circuit 117 may execute a proof generation program, which is provided by the data source system 150 (or the data server 157) in advance, to utilize the proof key PK1 to generate a proof PF1 according to the received data to be verified. Alternatively, the control circuit 117 may, based on a proof generation rule pre-set by the data server 157, utilize the proof key PK1 to generate a proof PF1 according to the received data to be verified. In operations, the control circuit 117 may utilize the proof key PK1 to conduct various appropriate zero-knowledge proof algorithm operations on the one or more data to be verified provided by the data owner D1, so as to generate a corresponding proof PK1 whose contents are not possible to be interpreted by other devices. In the data read authority control system 100, only the block chain system 180 is able to utilize the corresponding zero-knowledge proof smart contract SC-ZKP to verify whether the proof PF1 is correct or not.

[0099] It can be appreciated from the foregoing elaborations that the proof PF1 is substantially generated based on one or more constraints that only the data owner D1 and the operating unit of the data source system 150 know the correct information. If the data to be verified provided by the data owner D1 are all correct, then the proof PF1 generated by the control circuit 117 can be utilized to prove the authenticity of the identity of the data owner D1.

[0100] As shown in FIG. 2, when the data owner D1 wants to activate the data authority control service of the data read authority control system 100, the data owner D1 may utilize the data owner device 110 to perform the operation 228. In this situation, the block chain system 180 correspondingly performs the operation 230.

[0101] In the operation 228, the control circuit 117 of the data owner device 110 generates an authorization service activation request, and utilizes the communication circuit 111 or the block chain computing circuit 113 to transmit the authorization service activation request to the block chain system 180.

[0102] In the operation 230, the block chain system 180 executes the aforementioned token management smart contract SC-TM according to the authorization service activation request to generate an authorization token corresponding to the data owner device 110 (or its corresponding data owner D1), and transfers the authorization token to the data owner device 110. In one embodiment, the token management smart contract SC-TM may further configure

one or more corresponding activity inspection parameters on the authorization token, such as a valid time-slots of use, an expiration period, a valid geographical region, a valid owner, and/or a valid source network address, or the like.

[0103] In this situation, the communication circuit 111 or the block chain computing circuit 113 of the data owner device 110 may perform the operation 302 of FIG. 3 to acquire the authorization token transferred from the block chain system 180, so that the data owner device 110 becomes a current owner of the authorization token.

[0104] In the operation 304, the control circuit 117 of the data owner device 110 may encrypt the data authorization policy agreed by the target user (e.g., the data owner D1 in this example) under the manipulation of the target user, so as to generate a corresponding encrypted data authorization policy. For example, the control circuit 117 may configure corresponding data authorization policy for the data service system 160 under the manipulation of the data owner D1. The aforementioned data authorization policy may comprise part of or all of multiple parameters such as an authorized target (e.g., the identification data of the data service system 160 in this example), an authorized data subject, an authorization content, an upper limit of authorization times, an authorization period, an authorization time limit, a geographical area where the data is located, an identification data of the data source system 150 that keeps the sensitive data (e.g., an address of a specific smart contract deployed by the data source system 150 in the block chain system 180), or the like.

[0105] In some embodiments, the control circuit 117 may configure corresponding data authorization policies for other data requesters. In operations, the control circuit 117 may utilize a predetermined encryption key to encrypt respective data authorization policy to generate a corresponding encrypted data authorization policy.

[0106] In practice, the control circuit 117 may utilize the same encryption key to encrypt different data authorization policies, or may respectively utilize different encryption keys to encrypt different data authorization policies.

[0107] In the operation 306, the control circuit 117 may utilize the communication circuit 111 or the block chain computing circuit 113 to use the authorization token to transmit the generated one or more encrypted data authorization policies to the block chain system 180. In addition, the control circuit 117 may utilize the communication circuit 111 or the block chain computing circuit 113 to transmit one or more target keys, which can be utilized to decrypt the one or more encrypted data authorization policies, to the block chain system 180 or the data service system 160 at appropriate time points.

[0108] In the operation 308, the block chain system 180 may record the one or more

encrypted data authorization policies transmitted from the data owner device 110 in the aforementioned authorization policy smart contract SC-PL, so as to be a current data authorization policy corresponding to the data owner device 110.

[0109] As can be appreciated from the foregoing descriptions, the encrypted data authorization policy generated by the data owner device 110 and comprising the data authorization policy would be recorded in the block chain system 180. As a result, only devices having a correct decryption key and having the authority to read the block chain system 180 can read the encrypted data authorization policy from the block chain system 180 and decrypt the encrypted data authorization policy. Such approach can significantly reduce the possibility of the data authorization policy configured by the data owner device 110 being stolen or being tampered with by malicious persons.

[0110] In the data read authority control system 100, the users corresponding to other data owner device (e.g., the data owner D2 corresponding to the data owner device 120) may adopt the aforementioned approach to utilize related data owner devices to encrypt the data authorization policies corresponding to the data service system 160 (or corresponding to the data service system 160 and other data requesters), so as to generate one or more corresponding encrypted data authorization policies, and to transmit the encrypted data authorization policies to the block chain system 180, so that the block chain system 180 records the encrypted data authorization policies in the authorization policy smart contract SC-PL.

[0111] In practice, the block chain system 180 may create a single authorization policy smart contract SC-PL, and record the multiple encrypted data authorization policies generated by different data owners in the same authorization policy smart contract SC-PL.

[0112] Alternatively, the block chain system 180 may create different authorization policy smart contracts SC-PL respectively for different data requesters. For example, the block chain system 180 may create a dedicated authorization policy smart contract SC-PL for the data owner D1 to record one or more encrypted data authorization policies generated by the data owner D1, and may create another different authorization policy smart contract SC-PL for the data owner D2 to record one or more encrypted data authorization policies generated by the data owner D2.

[0113] In the operation 310, the control circuit 117 of the data owner device 110 may utilize the communication circuit 111 to transmit the aforementioned target data and proof PF1 to the data service system 160. In practice, the control circuit 117 may utilize the communication circuit 111 to transmit the target data and the proof PF1 to the data service system 160 at the same time point. Alternatively, the control circuit 117 may utilize the communication circuit

111 to respectively transmit the target data and the proof PF1 to the data service system 160 at different time points.

[0114] In this situation, the communication circuit 161 of the data service system 160 may perform the operation 312 to receive the target data and the proof PF1 transmitted from the data owner device 110. The web server 167 may store the target data received by the communication circuit 161 in the database 165.

[0115] In some embodiments, the control circuit 117 of the data owner device 110 may also utilize the communication circuit 111 to transmit the identification data of the verification key VK1 corresponding to the data owner D1 to the data service system 160. In this situation, the communication circuit 161 of the data service system 160 may receive the identification data of the verification key VK1 transmitted from the data owner device 110.

[0116] In practice, the control circuit 117 may utilize the communication circuit 111 to transmit the target data and the proof PF1 to the data service system 160 at the same time point. Alternatively, the control circuit 117 may utilize the communication circuit 111 to respectively transmit the target data and the proof PF1 to the data service system 160 at different time points.

[0117] As shown in FIG. 3, after receiving the target data and the proof PF1 transmitted from the data owner device 110, the data service system 160 may cooperate with the block chain system 180 to verify the authenticity of all or part of the target data.

[0118] For example, in the operation 314, the web server 167 may utilize the communication circuit 161 or the block chain computing circuit 163 to transmit the proof PF1 generated by the data owner device 110 to the block chain system 180, and to transmit a proof verification request to the block chain system 180, so as to request the block chain system 180 to verify the proof PF1. In some embodiments, the aforementioned proof verification request may comprise an identification data corresponding to the data owner device 110, an identification data corresponding to the data owner D1, or an identification data corresponding to the verification key VK1 of the data owner D1.

[0119] In the operation 316, the block chain system 180 may receive the proof PF1 and related proof verification request transmitted from the data service system 160.

[0120] In the operation 318, the block chain system 180 may execute a corresponding zero-knowledge proof smart contract SC-ZKP to verify the correctness of the proof PF1. For example, the block chain system 180 may locate the corresponding zero-knowledge proof smart contract SC-ZKP according to the identification data of the data owner device 110, the identification data of the verification key VK1 corresponding to the data owner D1, and/or the identification data corresponding to the data owner D1. For another example, the block chain

system 180 may extract an identification data corresponding to the data owner device 110, an identification data corresponding to the data owner D1, or an identification data corresponding to the verification key VK1 of the data owner D1 from the proof verification request, and the block chain system 180 may locate the corresponding zero-knowledge proof smart contract SC-ZKP according to the extracted identification data. Then, the block chain system 180 may execute the zero-knowledge proof smart contract SC-ZKP to find the corresponding verification key VK1 according to the aforementioned identification data, and to utilize the verification key VK1 to conduct an appropriate zero-knowledge proof verification algorithm operation on the proof PF1, so as to determine whether the proof PF1 satisfies the aforementioned first predetermined verification rule, thereby verifying the correctness of the proof PF1.

[0121] It can be appreciated from the foregoing elaborations that the proof PF1 is substantially generated based on one or more constraints that only the data owner D1 and the operating unit of the data source system 150 know the correct information. Accordingly, the block chain system 180 may execute the zero-knowledge proof smart contract SC-ZKP to utilize the verification key VK1 to conduct an appropriate zero-knowledge proof verification algorithm operation on the proof PF1 to determine whether the proof PF1 satisfies all the constraints specified in the aforementioned first predetermined verification rule or not.

[0122] If all the data to be verified provided by the data owner D1 to the data owner device 110 are correct, then the zero-knowledge proof verification algorithm executed by the zero-knowledge proof smart contract SC-ZKP will obtain a result indicating that the proof PF1 satisfies all the constraints in the aforementioned first predetermined verification rule. In this situation, the block chain system 180 is enabled to determine that the proof PF1 is correct without interpreting the content of the proof PF1.

[0123] On the contrary, if the data to be verified provided by the data owner D1 to the data owner device 110 contain errors, then the zero-knowledge proof verification algorithm executed by the zero-knowledge proof smart contract SC-ZKP will obtain a result indicating that the proof PF1 does not satisfy all the constraints in the aforementioned first predetermined verification rule. In this situation, the block chain system 180 is enabled to determine that the proof PF1 is incorrect without interpreting the content of the proof PF1.

[0124] As shown in FIG. 3, if the block chain system 180 determines that the proof PF1 is incorrect, the block chain system 180 may perform the operation 320. On the contrary, if the block chain system 180 determines that the proof PF1 is correct, the block chain system 180 may perform the operation 322.

[0125] In the operation 320, the block chain system 180 may transmit a proof-failed notification to the data service system 160.

[0126] In the operation 322, the block chain system 180 may transmit a verification success notification to the data service system 160.

[0127] In the operation 324, the web server 167 of the data service system 160 may receive the proof-failed notification transmitted from the block chain system 180 through the communication circuit 161 or the block chain computing circuit 163.

[0128] In the operation 326, the web server 167 may notify the data owner device 110 through the communication circuit 161, so that the data owner D1 can know that the data to be verified provided by the data owner D1 has not passed the verification of the zero-knowledge proof mechanism.

[0129] In the operation 328, the web server 167 may receive the verification success notification transmitted from the block chain system 180 through the communication circuit 161 or the block chain computing circuit 163. When the verification success notification is received by the web server 167, it means that the proof PF1 generated by the data owner device 110 has passed the verification of the ZKP verification mechanism adopted by the block chain system 180. Accordingly, the web server 167 can determine, according to the verification result of the block chain system 180, that the identity authenticity of the data owner D1 who created the target data has passed the verification (that is, it means that the data owner D1 is really a loan applicant who has applied for a housing loan to the operating unit of the data source system 150), and therefore can further determine that the total borrowing amount in the target data is an information supported by a factual basis.

[0130] In this situation, the web server 167 may perform the operation 330 to mark the target data. For example, the web server 167 may assign an identifiable symbol, pattern, annotated text, label, or prominent marking to the target data to mark the target data. In practical applications, the web server 167 may display the aforementioned mark when displaying the target data, so that the person who browses the target data is enabled to know that the authenticity of all or a part of the target data has passed the verification.

[0131] For another example, the web server 167 may assign the target data to a specific data category, so that the person who browses the target data is enabled to know that the authenticity of all or part of the target data has passed the verification of the block chain system 180.

[0132] In some embodiments, the web server 167 may store the target data transmitted from the data owner device 110 in the database 165 after receiving the verification success notification transmitted from the block chain system 180. In this situation, the aforementioned

operation 330 may be omitted.

[0133] As described previously, in some embodiments, the aforementioned first predetermined verification rule may contain a constraint that requires that a difference obtained by subtracting an approved loan amount from a house price should be equal to a predetermined loan gap amount. In this situation, the proof verification request transmitted from the web server 167 to the block chain system 180 in the operation 314 may further comprise a total borrowing amount specified in the target data. On the other hand, when the block chain system 180 executes the zero-knowledge proof smart contract SC-ZKP in the aforementioned operation 318, the zero-knowledge proof smart contract SC-ZKP may configure the total borrowing amount transmitted from the web server 167 to be the predetermined loan gap amount of the above constraint, and utilize the verification key VK1 to conduct an appropriate zero-knowledge proof verification algorithm operation on the proof PF1 to determine whether the proof PF1 satisfies all the constraints in the first predetermined verification rule.

[0134] As can be appreciated from the foregoing elaborations, if all the data to be verified provided by the data owner D1 are correct, then the zero-knowledge proof verification algorithm executed by the zero-knowledge proof smart contract SC-ZKP will obtain a result indicating that the proof PF1 satisfies all the constraints in the aforementioned first predetermined verification rule. As a result, the block chain system 180 is enabled to determine that the proof PF1 is correct without interpreting the content of the proof PF1.

[0135] In this situation, the web server 167 is enabled to further confirm the correctness of the total borrowing amount in the target data created by the data owner D1 according to the verification result of the block chain system 180.

[0136] It can be appreciated from the foregoing elaborations that when the data owner D1 encounters the home loan gap/housing loan gap problem, the data owner D1 may manipulate the data owner device 110 to log in to the data service system 160 to create description data (i.e., the aforementioned target data) of a home-loan-gap/housing-loan-gap lending case, to thereby initiate a home-loan-gap/housing-loan-gap lending activity. The data service system 160 may request the block chain system 180 to verify the proof PF1, which is generated by the data owner device 110 and corresponding to the target data, after receiving the target data transmitted from the data owner device 110, so as to verify the authenticity of the target data.

[0137] The block chain system 180 may execute the zero-knowledge proof smart contract SC-ZKP deployed by the data source system 150 to verify the correctness of the proof PF1 by adopting the ZKP verification mechanism. The data service system 160 may verify the authenticity of all or part of the content of the target data according to the verification result of

the proof PF1 conducted by the block chain system 180.

[0138] During the operation that the block chain system 180 executes the zero-knowledge proof smart contract SC-ZKP to verify the proof PF1, the data service system 160 does not need to provide the block chain system 180 with too much information about the data owner D1 (e.g., the house price and the approved loan amount). In this way, the amount of information required by the block chain system 180 for verifying the proof PF1 can be minimized, thereby greatly reducing the possibility that the relevant data of the data owner D1 to be leaked.

[0139] In addition, during the operation that the block chain system 180 executes the zero-knowledge proof smart contract SC-ZKP to verify the proof PF1, the block chain system 180 does not need to interact with either the data owner device 110 or the data source system 150, so the operating loading of the data owner device 110 and the data source system 150 will not be increased. Such an approach can also effectively reduce the involvement of the data owner D1 or the operating unit of the data source system 150, thereby reducing the risk of sensitive data leakage by the data owner D1 or the operating unit of the data source system 150.

[0140] On the other hand, when the investor party (or the lender party) wants to know whether there is any home-loan-gap/housing-loan-gap lending activity initiated by the borrower party on the data service system 160, the investor party can manipulate the corresponding data requester device to log in to the data service system 160. For illustrative purpose, it is assumed hereinafter that the aforementioned investor party is the data requester R1 corresponding to the data requester device 130.

[0141] When the data requester R1 wants to know whether there is any home-loan-gap/housing-loan-gap lending activity initiated by the borrower party on the data service system 160, the data requester R1 may manipulate the corresponding data requester device 130 to log in to the data service system 160.

[0142] In this situation, the control circuit 135 of the data requester device 130 may perform the operation 402 of FIG. 4 to utilize the communication circuit 131 to transmit a data browsing request to the data service system 160.

[0143] In this situation, the web server 167 of the data service system 160 may perform the operation 404 to receive the data browsing request transmitted from the data requester device 130 through the communication circuit 161.

[0144] In the operation 406, the web server 167 may utilize the communication circuit 161 to transmit one or more candidate data including the aforementioned target data created by the data owner D1 to the data requester device 130.

[0145] In the operation 408, the control circuit 135 may receive the candidate data transmitted from the data service system 160 through the communication circuit 131, and may control the display device 133 to display the candidate data. The data requester R1 can view the content of the candidate data to assess whether there are subject cases worthy of further study. It can be appreciated from the foregoing descriptions that the target data within the candidate data transmitted from the data service system 160 to the data requester device 130 is the description data of the home-loan-gap/housing-loan-gap lending case created by the data owner D1.

[0146] In general situations, the investor party may need to study certain further information or documents about the subject case before deciding whether to lend to the borrower party corresponding to the subject case. For example, the aforementioned sensitive data (e.g., the aforementioned credit evaluation reports, assessment reports, and/or loan contract documents/loan contract draft documents) related to individual loan applicants and stored in the database 155 of the data source system 150 may be auxiliary data worthy of further reading and research by the investor party when evaluating related home-loan-gap/housing-loan-gap lending case.

[0147] For the convenience of elaboration purpose, it is assumed hereinafter that the data requester R1 is interested in the home-loan-gap/housing-loan-gap lending case corresponding to the target data, and therefore wants to obtain specific sensitive data stored in the data source system 150 and corresponding to the target data (e.g., the credit evaluation reports, assessment reports, and/or loan contract documents/loan contract draft documents related to the data owner D1) for further reading and research.

[0148] In this situation, the data requester R1 may issue a selection command corresponding to the target data to the data requester device 130 through various suitable input interfaces (not shown in the figure). At this time, the control circuit 135 of the data requester device 130 may perform the operation 410 to generate a sensitive data request corresponding to the target data. The aforementioned sensitive data request can be utilized for requesting certain specific sensitive data (e.g., the credit evaluation reports, assessment reports, and/or loan contract documents/loan contract draft documents related to the data owner D1) of the home-loan-gap/housing-loan-gap lending case corresponding to the target data.

[0149] In the operation 412, the control circuit 135 may utilize the communication circuit 131 to transmit the sensitive data request to the data service system 160.

[0150] In the operation 414, the web server 167 may receive the sensitive data request transmitted from the data requester device 130 through the communication circuit 161.

[0151] In this embodiment, the web server 167 will not immediately provide the corresponding sensitive data to the data requester device 130 after receiving the sensitive data request transmitted from the data requester device 130. Instead, the web server 167 would further check whether the data requester device 130 has a corresponding data read authority. Therefore, the web server 167 may perform the operation 416 after receiving the sensitive data request transmitted from the data requester device 130.

[0152] In the operation 416, the web server 167 may generate a data read request corresponding to a target requester (e.g., the data requester R1 in this example) and the aforementioned sensitive data request, and may utilize the communication circuit 161 or the block chain computing circuit 163 to transmit the data read request to the data owner device 110 corresponding to the data owner D1.

[0153] In the operation 418, the control circuit 117 of the data owner device 110 may receive the data read request transmitted from the data service system 160 through the communication circuit 111 or the block chain computing circuit 113.

[0154] In the operation 420, the control circuit 117 may adopt a suitable mechanism to inquire the target user (e.g., the data owner D1 in this example) whether to accept the data read request transmitted from the data service system 160.

[0155] For example, the control circuit 117 may control the display device 115 to display a query screen including relevant information of the data read request, so as to ask the data owner D1 whether to accept the data read request. For another example, the control circuit 117 may control a sound generating circuit (not shown in the figure) of the data owner device 110 to generate a related voice prompt message to ask the data owner D1 whether to accept the data read request.

[0156] If the data owner D1 rejects the data read request transmitted from the data service system 160, the data owner device 110 may perform the operation 422. On the contrary, if the data owner D1 accepts the data read request transmitted from the data service system 160, the data owner device 110 may perform the operation 424.

[0157] In the operation 422, the control circuit 117 may utilize the communication circuit 111 or the block chain computing circuit 113 to transmit a rejection notice to the data service system 160.

[0158] In the operation 424, the control circuit 117 may utilize the communication circuit 111 or the block chain computing circuit 113 to transmit an identification data of the authorization token corresponding to the data owner device 110 (hereinafter referred to an authorization token identification data) to the data service system 160.

[0159] In the operation 426, the web server 167 may receive the rejection notice transmitted from the data owner device 110 through the communication circuit 161 or the block chain computing circuit 163, and utilize the communication circuit 161 to transmit a corresponding rejection message to the data requester device 130.

[0160] In the operation 428, the control circuit 135 may receive the rejection message transmitted from the data service system 160 through the communication circuit 131, and control the display device 133 to display the rejection message, so that the data requester R1 is enabled to know the relevant information.

[0161] In the operation 430, the web server 167 may receive the authorization token identification data transmitted from the data owner device 110 through the communication circuit 161 or the block chain computing circuit 163.

[0162] It can be appreciated from the foregoing elaborations that when the authorization token identification data transmitted from the data owner device 110 is received by the web server 167, it means that the data owner D1 accepted the data read request generated by the data service system 160. Accordingly, the web server 167 may perform the operation 432 to generate a read token request comprising the authorization token identification data corresponding to the data owner device 110, and may utilize the communication circuit 161 or the block chain computing circuit 163 to transmit the read token request to the block chain system 180. The aforementioned read token request is utilized for requesting the block chain system 180 to provide a read token corresponding to specific sensitive data related to the target data.

[0163] In this situation, the block chain system 180 may perform the operation 502 of FIG. 5 to receive the read token request transmitted from the data service system 160. Please note that after receiving the read token request transmitted from the data service system 160, the block chain system 180 will not immediately provide a corresponding read token to the data service system 160. Instead, the block chain system 180 would further check whether the data service system 160 has a corresponding data read authority.

[0164] In the operation 504, the block chain system 180 may execute the authorization policy smart contract SC-PL to inspect whether the read token request complies with the predetermined authorization policy or not. In operations, the block chain system 180 may obtain a corresponding authorization token identification data based on the read token request. Since only the data owner device 110 has the authority to use the authorization token corresponding to the authorization token identification data, the block chain system 180 may locate and retrieve the encrypted data authorization policy generated by the data owner device

110 from the authorization policy smart contract SC-PL according to the authorization token identification data.

[0165] The block chain system 180 may utilize the aforementioned target key to decrypt the encrypted data authorization policy to acquire the decrypted data authorization policy. Then, the block chain system 180 may determine whether the read token request complies with the requirements of the data authorization policy configured by the data owner D1 or not according to the contents of the decrypted data authorization policy.

[0166] If the data service system 160 is not an authorized target indicated by the decrypted data authorization policy, or the specific sensitive data corresponding to the read token request does not belong to the authorized data subject, then the block chain system 180 may determine that the read token request does not comply with the data authorization policy configured by the data owner D1. In this situation, the block chain system 180 may perform the operation 506.

[0167] On the contrary, if the data service system 160 is an authorized target indicated by the decrypted data authorization policy, and the specific sensitive data corresponding to the read token request belongs to the authorized data subject, then the block chain system 180 may determine that the read token request complies with the data authorization policy configured by the data owner D1. In this situation, the block chain system 180 may perform the operation 510.

[0168] In the operation 506, the block chain system 180 may generate and transmit a non-qualification notice to the data service system 160. In this situation, the web server 167 may perform the operation 508 to receive the non-qualification notice transmitted from the block chain system 180 through the communication circuit 161 or the block chain computing circuit 163, and to accordingly reject the sensitive data request issued by the data requester device 130.

[0169] In the operation 510, the block chain system 180 may execute the token management smart contract SC-TM to verify the activity of an authorization token corresponding to the authorization token identification data. For example, the token management smart contract SC-TM may inspect whether related parameters of the authorization token match the validity inspection parameters configured by the token management smart contract SC-TM in the aforementioned operation 230.

[0170] In one embodiment, the token management smart contract SC-TM may determine the authorization token as an inactive token if some parameters of the authorization token do not match the validity inspection parameters configured in the aforementioned operation 230. In another embodiment, the token management smart contract SC-TM determines the

authorization token as inactive only if all of the parameters of the authorization token do not match the validity inspection parameters configured in the aforementioned operation 230, otherwise the token management smart contract SC-TM determines the authorization token as an active token.

[0171] If the token management smart contract SC-TM determines the authorization token is an inactive token, then the token management smart contract SC-TM performs the operation 512. On the contrary, if the token management smart contract SC-TM determines the authorization token is an active token, then the token management smart contract SC-TM performs the operation 518.

[0172] In the operation 512, the token management smart contract SC-TM may generate and transmit an authorization token inactive notice to the data service system 160. At this time, the web server 167 may perform the operation 514 to receive the authorization token inactive notice from the communication circuit 161 or the block chain computing circuit 163. In this situation, the web server 167 may perform the operation 516 to reject the sensitive data request issued by the data requester device 130.

[0173] In the operation 518, the token management smart contract SC-TM may generate and transfer a read token corresponding to the authorization token to the data service system 160. In operations, the token management smart contract SC-TM may configure a corresponding expiration period for the read token, such as5 days, 10 days, 1 week, 2 weeks, 1 month, or the like. The expiration period configured by the token management smart contract SC-TM for the read token will be equal to or shorter than the expiration period of the authorization token. In practice, the token management smart contract SC-TM may create an appropriate data association or activity association between the read token and the authorization token, and may deactivate the read token when the authorization token becomes inactive.

[0174] In the operation 520, the web server 167 may acquire the read token transferred from the block chain system 180 through the communication circuit 161 or the block chain computing circuit 163.

[0175] In the operation 522, the web server 167 may utilize the communication circuit 161 or the block chain computing circuit 163 to transmit a sensitive data request to the data source system 150, and transfer the read token to the data source system 150. The aforementioned sensitive data request can be utilized for requesting certain specific sensitive data (e.g., the credit evaluation reports, assessment reports, and/or loan contract documents/loan contract draft documents related to the data owner D1) of the home-loan-gap/housing-loan-gap lending

case corresponding to the target data. In practice, the sensitive data request transmitted from the data service system 160 to the data source system 150 in the operation 522 may be identical to the sensitive data request received by the data service system 160 in the operation 414, or may be different in the data format or other aspects that do not affect its main function.

[0176] In this situation, the data source system 150 may perform the operation 524.

[0177] In the operation 524, the data server 157 may receive the sensitive data request transmitted from the data service system 160 through the communication circuit 151 or the block chain computing circuit 153, and acquire the read token transferred from the data service system 160.

[0178] Please note that the block chain system 180 may swap the order of the determining operations of the aforementioned operation 504 and operation 510. In other words, after receiving the read token request transmitted from the data service system 160, the block chain system 180 may perform the operation 510 first, and then perform the operation 504 if determining the authorization token as an active token. In this situation, the block chain system 180 may perform the aforementioned operation 518 after determining the read token as an active token in the operation 504.

[0179] As can be appreciated from the foregoing descriptions of FIG. 5, the token management smart contract SC-TM generates the read token having an association with the authorization token and transfers the read token to the data service system 160 only in the situation where the authorization token corresponding to the data owner D1 is determined as an active token by the token management smart contract SC-TM.

[0180] In other words, if the block chain system 180 deactivates the authorization token corresponding to the data owner device 110 due to various reasons (e.g., the data owner D1 terminates the service of the data read authority control system 100, or the data owner D1 is suspended), then the block chain system 180 will no longer provide the read token for reading related sensitive data of the data owner D1 to the data service system 160 or other data requesters. Obviously, such mechanism can avoid the possibility of improper access to the related sensitive data of the data owner D1, which is beneficial in improving the protection level for the related sensitive data of the data owner D1.

[0181] In addition, the token management smart contract SC-TM would generate the read token having an association with the authorization token and transfer the read token to the data service system 160 only in the situation that the block chain system 180 determines that the read token request complies with the data authorization policy configured by the data owner D1. Accordingly, even if the read token request generated by the data service system 160 is

intercepted by other malicious devices that do not comply with the data authorization policy, the block chain system 180 will not transfer the read token to these malicious devices.

[0182] Please note that the data source system 150 will not immediately provide the corresponding sensitive data to the data service system 160 after receiving the sensitive data request transmitted from the data service system 160. Instead, the data source system 150 requests the block chain system 180 to verify the activity of the read token to determine whether the data service system 160 has a corresponding data read authority.

[0183] Therefore, the data source system 150 may perform the operation 602 of FIG. 6 after performing the operation 524.

[0184] In the operation 602, the data server 157 may utilize the communication circuit 151 or the block chain computing circuit 153 to transfer the read token to the block chain system 180, and request the block chain system 180 to verify the activity of the read token. In this situation, the block chain system 180 may corresponding perform the operation 604.

[0185] In the operation 604, the block chain system 180 may acquire the read token transferred from the data source system 150.

[0186] Then, the block chain system 180 may perform the operation 606 to execute the token management smart contract SC-TM to verify the activity of the read token. As described previously, the token management smart contract SC-TM may set a corresponding expiration period for the read token in the aforementioned operation 518. Accordingly, in the operation 606, the token management smart contract SC-TM may inspect whether a time point at which the block chain system 180 acquires the read token has exceeded the expiration period configured in the operation 518 or not.

[0187] If a time point at which the block chain system 180 acquires the read token has exceeded the expiration period configured by the token management smart contract SC-TM in the operation 518, then the token management smart contract SC-TM determines the read token as an inactive token and performs the operation 608.

[0188] On the contrary, if a time point at which the block chain system 180 acquires the read token does not exceed the expiration period configured by the token management smart contract SC-TM in the operation 518, then the token management smart contract SC-TM determines the read token as an active token and performs the operation 614.

[0189] In another embodiment, when the block chain system 180 executes the token management smart contract SC-TM to verify the activity of the read token, the block chain system 180 would inspect whether the read token is transferred from the data service system 160 to the data source system 150 before being transferred to the block chain system 180, and

also inspect whether a time point at which the read token is transferred from the data source system 150 to the block chain system 180 has exceeded the expiration period or not. In this embodiment, the token management smart contract SC-TM determines the read token as an active token and perform the operation 614 only in the situation where the time point at which the block chain system 180 acquires the read token does not exceed the expiration period and the read token is transferred from the data service system 160 to the data source system 150 before being transferred to the block chain system 180. Otherwise, the token management smart contract SC-TM would determine the read token as an inactive token and performs the operation 608.

[0190] In the operation 608, the token management smart contract SC-TM may generate and transmit a verification failure notice to the data source system 150. In this situation, the data server 157 may corresponding perform the operation 610 to receive the verification failure notice through the communication circuit 151 or the block chain computing circuit 153. Then, the data server 157 may perform the operation 612 to reject the sensitive data request transmitted from the data service system 160, and may utilize the communication circuit 151 or the block chain computing circuit 153 to transmit a corresponding rejection notice to the data service system 160.

[0191] In the operation 614, the token management smart contract SC-TM may generate and transmit a verification success notice to the data source system 150, and may optionally deactivate the read token. In this situation, the data server 157 may corresponding perform the operation 616 to receive the verification success notice through the communication circuit 151 or the block chain computing circuit 153.

[0192] In the operation 618, the data server 157 may find out the sensitive data corresponding to the target data (e.g., the credit evaluation reports, assessment reports, and/or loan contract documents/loan contract draft documents related to the data owner D1) from multiple sensitive data stored in the database 155, and may utilize the communication circuit 151 or the block chain computing circuit 153 to transmit the sensitive data corresponding to the target data to the data service system 160. In this situation, the web server 167 may corresponding perform the operation 620 to receive the sensitive data transmitted from the data source system 150 through the communication circuit 161 or the block chain computing circuit 163. In addition, the web server 167 may further utilize the communication circuit 151 or the block chain computing circuit 153 to transmit the sensitive data to the data requester device 130.

[0193] In this situation, the control circuit 135 of the data requester device 130 may perform

the operation 622 to receive the sensitive data transmitted from the data service system 160 through the communication circuit 131.

[0194] In the operation 624, the control circuit 135 may control the display device 133 to display the sensitive data corresponding to the target data (e.g., the credit evaluation reports, assessment reports, and/or loan contract documents/loan contract draft documents related to the data owner D1). As a result, the data requester R1 is enabled to research the aforementioned sensitive data to assess whether to lend money to the borrower party in a specific home-loan-gap/housing-loan-gap lending case (i.e., the data owner D1 corresponding to the target data in this embodiment).

[0195] After the data requester R1 decides to lend money to the data owner D1, the data service system 160 may adopt various existing appropriate mechanisms to assist the data requester R1 and the data owner D1 to realize related information flow and/or financial flow operations.

[0196] In practical applications, the data service system 160 may adopt various existing appropriate mechanisms to match the borrowing needs of different borrower parties and the investment needs of different investor parties, so as to assist more borrower parties to borrow required money through the data service system 160.

[0197] On the other hand, as shown in FIG. 6, after determining the read token as an active token, the token management smart contract SC-TM may further perform the operation 626 to record an acquisition time of the read token (e.g., an occurrence time of the operation 604), or a verification time of the read token (e.g., an occurrence time of the operation 606 or of the operation 614).

[0198] The related temporal data of the read token recorded by the block chain system 180 in the operation 626 may be utilized to be the supporting evidence for proving that the data source system 150 provides the related sensitive data of the data owner D1 to the data service system 160.

[0199] As can be appreciated from the foregoing descriptions of FIG. 6, the data source system 150 provides the sensitive data corresponding to the sensitive data request to the data service system 160 only in the situation that the token management smart contract SC-TM also determines the read token as an active token.

[0200] In other words, as long as the read token is inactive, the data source system 150 would not provide the related sensitive data of the data owner D1 to the data service system 160. Therefore, the aforementioned approach adopted by the data source system 150 to utilize the block chain system 180 to verify the activity of the read token can effectively avoid the

possibility of improper access to the related sensitive data of the data owner D1, which is beneficial in significantly improving the protection level for the related sensitive data of the data owner D1.

[0201] In addition, based on the characteristics of the block chain system 180, the related temporal data of the read token recorded in the block chain system 180 is difficult to be tampered with, thus the aforementioned related temporal data may be utilized as the supporting evidence for proving that the data source system 150 did provide the related sensitive data of the data owner D1 to the data service system 160, which is beneficial in reducing the possibility of disputes between the data source system 150 and the data service system 160 that are difficult to clarify.

[0202] Furthermore, each time the data service system 160 provides the sensitive data to a data requester device, a corresponding time record of the corresponding read token will theoretically be generated on the block chain system 180. Such mechanism also helps to avoid the possibility that the data service system 160 leaks the sensitive data of the data owner without authorization to those who do not have the right to access the data.

[0203] In practice, in addition to transfer the read token to the block chain system 180, the data source system 150 may also transmit the sensitive data request transmitted from the data service system 160 to the block chain system 180 and request the block chain system 180 to verify the validity of the sensitive data request.

[0204] For example, the data server 157 may utilize the communication circuit 151 or the block chain computing circuit 153 to transmit the sensitive data request to the block chain system 180, and request the block chain system 180 to execute the authorization policy smart contract SC-PL to inspect whether the sensitive data request complies with the predetermined authorization policy.

[0205] Since the read token corresponds to the authorization token that only the data owner device 110 has the authority to use, the block chain system 180 may locate and retrieve the encrypted data authorization policy generated by the data owner device 110 from the authorization policy smart contract SC-PL.

[0206] The block chain system 180 may utilize the aforementioned target key to decrypt the encrypted data authorization policy, so as to acquire the decrypted data authorization policy. Then, the block chain system 180 may determine whether the sensitive data request complies with the data authorization policy configured by the data owner D1 or not according to the contents of the decrypted data authorization policy.

[0207] If the specific sensitive data corresponding to the sensitive data request belong to the

authorized data subject, then the block chain system 180 may determine the sensitive data request as a valid data request.

[0208] On the contrary, if the specific sensitive data corresponding to the sensitive data request do not belong to the authorized data subject, then the block chain system 180 may determine the sensitive data request as an invalid data request.

[0209] In one embodiment, the block chain system 180 may inspect whether the sensitive data request is a valid data request or not by adopting the aforementioned approach before performing the operation 606, and perform the operation 606 only if the sensitive data request is determined as a valid data request. In this situation, if the block chain system 180 determines the sensitive data request as an invalid data request, the block chain system 180 may then perform the operation 608.

[0210] In another embodiment, the block chain system 180 may perform the operation 606 first, and after determining the read token as an active token, the block chain system 180 may inspect whether the sensitive data request is a valid data request or not by adopting the aforementioned approach. In this embodiment, the block chain system 180 would perform the operation 614 only in the situation that the sensitive data request is determined as a valid data request. If the block chain system 180 determines the sensitive data request as an invalid data request, the block chain system 180 may perform the operation 608.

[0211] As a result, the data source system 150 would provide the sensitive data corresponding to the sensitive data request to the data service system 160 only in the situation where the block chain system 180 determines the sensitive data request as a valid data request and the token management smart contract SC-TM also determines the read token as an active token.

[0212] In other words, if the sensitive data request is invalid or the read token is inactive, the data source system 150 will not provide related sensitive data of the data owner D1 to the data service system 160.

[0213] Therefore, the aforementioned approach adopted by the data source system 150 to utilize the block chain system 180 to verify the validity of the sensitive data request and the activity of the read token can effectively avoid the possibility of improper access to the related sensitive data of the data owner D1, which is beneficial in significantly improving the protection level for the related sensitive data of the data owner D1.

[0214] In some embodiments, the data read token used by the data service system 160 at each time is deactivated by the block chain system 180 in the end. This is equivalent to that these data read tokens in the end are collected by the block chain system 180, rather than the

data source system 150. Such structure can effectively reduce the possibility of disputes between the data source system 150 and the data service system 160.

[0215] The data requester R1 may utilize the data requester device 130 to request the data service system 160 to provide related sensitive data of other data owners (e.g., the data owner D2) by adopting the aforementioned approach as described in FIG. 4 through FIG. 6.

[0216] In the data read authority control system 100, other data requester devices (e.g., the data requester device 140 corresponding to the data requester R2) may adopt the aforementioned approach to utilize corresponding data requester device to request the data service system 160 to provide the related sensitive data of the data owner D1 (or other data owners).

[0217] Similarly, the data service system 160 may utilize the block chain system 180 to verify the data read authority of related data requester device, so as to prevent the sensitive data of the data owner from being easily leaked.

[0218] In the data read authority control operations conducted by the data read authority control system 100 described previously, operations needed to be performed by the data source system 150 are obviously much less than operations needed to be performed by the data service system 160. In addition, before the data source system 150 provides the sensitive data of respective data owner to the data service system 160, related data request or read token request needs to be verified by the block chain system 180 or even by the related data owner device. Such an approach can effectively justify the operation that the data source system 150 provides the sensitive data of individual data owner to the data service system 160.

[0219] Therefore, from another aspect, the system operating loading of the data source system 150 and the related data read authority inspection burden can be greatly reduced by adopting the aforementioned data read authority control method.

[0220] As can be appreciated from the foregoing elaborations, during the process that the borrower party initiates the home-loan-gap/housing-loan-gap lending activity to the investor parties through the data service system 160, the data service system 160 can not only facilitate the matching of the needs of the borrower party and the lender parties, but also cooperate with the block chain system 180 to effectively control the read authority of the sensitive data of the borrower party. Apparently, the data service system 160 plays a very important role in the online home-loan-gap/housing-loan-gap lending matching application described above.

[0221] As a result, in the applications where the data source system 150 and the data service system 160 belong to different operation entities, the data read authority control operations conducted by the cooperation of the data service system 160 and the block chain system 180

can significantly reduce the legal responsibility that the operation entity of the data source system 150 needs to undertake. Such a mechanism is beneficial in promoting the development of online home-loan-gap/housing-loan-gap lending matching applications.

[0222] As can be appreciated from the foregoing descriptions, historical versions of the encrypted data authorization policy comprising the data authorization policy and generated by the data owner device 110 are recorded in the block chain system 180. A device having a correct decryption key and having the authority to read the block chain system 180 can read the historical versions of the encrypted data authorization policy configured by the data owner D1 from the block chain system 180 and decrypt the historical versions of the encrypted data authorization policy. Such mechanism can ensure that the data authorization policy of the data owner has sufficient confidentiality, and can also enhance the transparency of the data owner's data authorization policy to interested parties. It is a balanced architecture that is ideal for both sides and will not be too biased towards either party.

[0223] Respective data owners can utilize their respective data owner devices to dynamically adjust the data read authority of the data service system 160 or other data service providers. In other words, individual data owners are enabled to flexibly adjust the data scope, data type, and/or data content that they are willing to authorize the data service system 160 or other data service providers to read.

[0224] As can be appreciated from the foregoing elaborations, after receiving the target data transmitted from the data owner device 110, the data service system 160 can request the block chain system 180 to verify the proof PF1 that is generated by the data owner device 110 and corresponds to the target data, so as to thereby verify the authenticity of the target data.

[0225] The block chain system 180 may execute the zero-knowledge proof smart contract SC-ZKP deployed by the data source system 150 to verify the correctness of the proof PF1 by adopting the ZKP verification mechanism. The data service system 160 may verify the authenticity of all or part of the content of the target data according to the verification result of the proof PF1 conducted by the block chain system 180.

[0226] During the operation that the block chain system 180 executes the zero-knowledge proof smart contract SC-ZKP to verify the proof PF1, the data service system 160 does not need to provide the block chain system 180 with too much information about the data owner D1. In this way, the amount of information required by the block chain system 180 for verifying the proof PF1 can be minimized, thereby greatly reducing the possibility that the relevant data of the data owner D1 to be leaked.

[0227] In addition, during the operation that the block chain system 180 executes the zero-

knowledge proof smart contract SC-ZKP to verify the proof PF1, the block chain system 180 does not need to interact with either the data owner device 110 or the data source system 150, and thus the operating loading of the data owner device 110 and the data source system 150 will not be increased. Such an approach can also effectively reduce the involvement of the data owner D1 or the operating unit of the data source system 150, thereby reducing the risk of sensitive data leakage by the data owner D1 or the operating unit of the data source system 150.

[0228] Devices having the authority to read the block chain system 180 and having a correct decryption key can decrypt and inspect the encrypted data authorization policy recorded in the block chain system 180. Therefore, adopting the block chain system 180 to replace the traditional centralized authorization server effectively improves the transparency of the data read authority control system 100 in terms of authorization policy management, thereby reducing the possibility of disputes between the data source system 150 and the data owners or between the data source system 150 and the data requesters.

[0229] Another advantage of the disclosed data read authority control system 100 is that it meets various GDPR requirements of the EU, and is enabled to permit the data owners to dynamically adjust their data authorization policies as needed at any time, which provides higher flexibility in adjusting authorization policies.

[0230] In addition, the data authorization policies of individual data owners are stored in the block chain system 180 in encrypted form, and only devices having a correct decryption key and having the authority to read the block chain system 180 can read the related encrypted data authorization policy from the block chain system 180 and decrypt the related encrypted data authorization policy. Such approach can significantly reduce the possibility of the data authorization policy configured by individual data owners being stolen or being tampered with by malicious persons.

[0231] Furthermore, the data read token used by the data service system 160 at each time is deactivated by the block chain system 180 in the end. This is equivalent to that these data read tokens in the end are collected by the block chain system 180, rather than the data source system 150. Such structure can effectively reduce the possibility of disputes between the data source system 150 and the data service system 160.

[0232] On the other hand, the authorization read authority control method adopted by the data read authority control system 100 utilizes the block chain system 180 to cooperate with related smart contracts to automatically complete the requesting procedure and transferring procedure of the data read token, the activity verification procedure of the authorization token, the validity verification procedure of the sensitive data request, and the activity verification

procedure of the read token. Therefore, the efficiency and correctness of the data read authority control operations can be significantly improved, and at the same time the required manpower and time are significantly reduced, and can even effectively avoid the risk that the related encrypted authorization policies and the time records of the read tokens stored in the block chain system 180 being tampered with by malicious persons afterwards.

[0233] In practice, the quantity of the data owner devices, the quantity of the data requester devices, the quantity of the data source systems 150, and the quantity of the data service systems 160 in the data read authority control system 100 may be increased according to the needs of the practical application environment, rather than a restriction to the practical implementations.

[0234] In some embodiments, the block chain computing circuit 113 of the data owner device 110 may be omitted. Alternatively, the display device 115 and/or the block chain computing circuit 113 may be arranged separately from the data owner device 110.

[0235] Additionally, in some embodiments, the display device 133 of the data requester device 130 may be arranged separately form the data requester device 130.

[0236] Similarly, in some embodiments, the database 155 and/or the block chain computing circuit 153 of the data source system 150 may be arranged separately form the data source system 150.

[0237] Please note that the executing order of the foregoing operations in each flowchart is merely an exemplary embodiment, rather than a restriction to the practical implementations. For example, the operation 212 and/or the operation 214 of FIG. 2 may be performed before the operation 210, or may be performed at the same time as the operations 210.

[0238] For another example, the operation 214 of FIG. 2 may be performed before the operation 212, or may be performed at the same time as the operation 212.

[0239] For yet another example, the operation 216 of FIG. 2 may be performed before the operation 206 or the operation 208, or may be performed at the same time as the operation 206 or the operation 208.

[0240] For yet another example, the operation 220, the operation 222, and the operation 224 of FIG. 2 may be performed before the operation 218.

[0241] For yet another example, the operation 228 and the operation 230 of FIG. 2 may be performed before the operation 218, the operation 220, the operation 222, the operation 224, or the operation 226.

[0242] For yet another example, the operation 310 and the operation 312 of FIG. 3 may be performed before the operation 302, the operation 304, or the operation 306.

[0243] For yet another example, the operation 304, the operation 306, and the operation 308 of FIG. 3 may be performed at any time point between the operation 312 and the operation 502.

[0244] For yet another example, in some embodiments, the control circuit 117 of the data owner device 110 may request the data owner D1 to input one or more data to be verified before the data owner D1 manipulates the data owner device 110 to log in to the data service system 160. And the control circuit 117 requests the data owner D1 to input some data of relatively high-sensitivity after the data owner D1 logged in the data service system 160. In other words, the data owner D1 may respectively input the data to be verified and the data of relatively high-sensitivity to the data owner device 110 at different time points. In this situation, the operation 226 may be performed before the operation 224.

[0245] For yet another example, in some embodiments, the data owner device 110 may transmit the authorization token identification data to the data service system 160 before performing the operation 416. For example, the data owner device 110 may transmit the authorization token identification data to the data service system 160 in the operation 310, or at other time point in advance. As a result, the operation 416 through the operation 430 of FIG. 4 may be omitted.

[0246] Certain terms are used throughout the description and the claims to refer to particular components. One skilled in the art appreciates that a component may be referred to as different names. This disclosure does not intend to distinguish between components that differ in name but not in function. In the description and in the claims, the term "comprise" is used in an open-ended fashion, and thus should be interpreted to mean "include, but not limited to." The term "couple" is intended to compass any indirect or direct connection. Accordingly, if this disclosure mentioned that a first device is coupled with a second device, it means that the first device may be directly or indirectly connected to the second device through electrical connections, wireless communications, optical communications, or other signal connections with/without other intermediate devices or connection means.

[0247] The term "and/or" may comprise any and all combinations of one or more of the associated listed items. In addition, the singular forms "a," "an," and "the" herein are intended to comprise the plural forms as well, unless the context clearly indicates otherwise.

[0248] Other embodiments of the invention will be apparent to those skilled in the art from consideration of the specification and practice of the invention disclosed herein. It is intended that the specification and examples be considered as exemplary only, with a true scope and spirit of the invention indicated by the following claims.

CLAIMS

What is claimed is:

1. A data read authority control system (100), comprising:

a block chain system (180);

a data owner device (110) arranged to operably receive data inputted by a target user to generate a target data, and to operably utilize a proof key to generate a proof;

a data source system (150) arranged to operably store a sensitive data corresponding to the target data;

a data service system (160) arranged to operably receive the target data and the proof generated by the data owner device (110), and to operably request the block chain system (180) to verify the proof;

a data requester device (130) arranged to operably generate and transmit a sensitive data request corresponding to the target data to the data service system (160);

wherein the block chain system (180) arranged to operably execute a zero-knowledge proof smart contract to utilize a verification key to verify correctness of the proof, and to operably transmit a verification success notification to the data service system (160) when the proof is determined as correct;

wherein the block chain system (180) is further arranged to operably verify an activity of an authorization token corresponding to an authorization token identification data, and to operably generate and transfer a read token to the data service system (160) when determining the authorization token as active;

wherein the data service system (160) is further arranged to operably transmit the sensitive data request to the data source system (150) and transfer the read token to the data source system (150) after acquiring the read token;

wherein if the read token transferred from the data service system (160) to the data source system (150) is active, the data source system (150) operably transmits the sensitive data corresponding to the target data to the data service system (160), and the data service system (160) operably transmits the sensitive data to the data requester device (130).

2. The data read authority control system (100) of claim 1, wherein the data service system (160) is further arranged to operably transmit the authorization token identification data to the

block chain system (180) after receiving the sensitive data request transmitted from the data requester device (130).

3. The data read authority control system (100) of claim 2, wherein the proof key utilized by the data owner device (110) and the verification key utilized by the block chain system (180) are both provided by the data source system (150).

4. The data read authority control system (100) of claim 2, wherein the data owner device (110) is further arranged to operably request the target user to input one or more data to be verified, and to operably utilize the proof key to generate the proof based on the one or more data to be verified.

5. The data read authority control system (100) of claim 2, wherein the authorization token is generated by the block chain system (180) and transferred to the data owner device (110).

6. The data read authority control system (100) of claim 5, wherein the block chain system (180) is further arranged to operably execute a token management smart contract to generate and transfer the authorization token to the data owner device (110);

wherein the data owner device (110) is further arranged to operably utilize the authorization token to transmit an encrypted data authorization policy to the block chain system (180), and the block chain system (180) is further arranged to operably record the encrypted data authorization policy in an authorization policy smart contract.

7. The data read authority control system (100) of claim 2, wherein the block chain system (180) is further arranged to operably execute an authorization policy smart contract to inspect whether the data service system (160) matches a predetermined authorization policy configured by the target user after receiving the authorization token identification data transmitted from the data service system (160).

8. The data read authority control system (100) of claim 7, wherein the block chain system (180) generates and transfers the read token to the data service system (160) only if the block chain system (180) determines that the authorization token is active and the data service system (160) matches the predetermined authorization policy.

9. The data read authority control system (100) of claim 2, wherein the data service system (160) is further arranged to operably generate and transmit a data read request corresponding to a target requester to the data owner device (110) after receiving the sensitive data request transmitted from the data requester device (130), and the data service system (160) transmits the authorization token identification data to the block chain system (180) only if the data read request is accepted by the target user.

10. The data read authority control system (100) of claim 9, wherein the data owner device (110) is further arranged to operably inquire the target user whether to accept the data read request, and to operably transmit the authorization token identification data to the data service system (160) if the data read request is accepted by the target user.

11. The data read authority control system (100) of claim 2, wherein the data source system (150) is further arranged to operably transfer the read token to the block chain system (180) after acquiring the read token;

wherein the block chain system (180) is further arranged to operably verify the activity of the read token after acquiring the read token, and to operably generate and transmit a verification success notice to the data source system (150) when determining the read token as active;

wherein the data source system (150) is further arranged to operably transmit the sensitive data corresponding to the target data to the data service system (160) after receiving the verification success notice.

12. The data read authority control system (100) of claim 11, wherein the block chain system (180) is further arranged to operably set a corresponding expiration period for the read token when generating the read token;

wherein when the block chain system (180) verifies the activity of the read token, the block chain system (180) inspects whether the read token is transferred by the data service system (160) to the data source system (150) before the read token is transferred to the block chain system (180), and the block chain system (180) further inspects whether a time point at which the data source system (150) transfers the read token to the block chain system (180) has exceeded the expiration period or not.

13. The data read authority control system (100) of claim 11, wherein the block chain system (180) is further arranged to operably records an acquisition time of the read token or a verification time of the read token.

14. A data service system (160) of a data read authority control system (100), wherein the data read authority control system (100) comprises a data owner device (110), a data requester device (130), a data source system (150), and a block chain system (180), the data service system (160) comprising:

a communication circuit (161) arranged to operably receive a target data and a proof transmitted from the data owner device (110), and to operably receive a sensitive data request corresponding to the target data transmitted from the data requester device (130);

a block chain computing circuit (163) arranged to operably act as one node of the block chain system (180), and arranged to operably request the block chain system (180) to verify the proof, wherein the block chain system (180) executes a zero-knowledge proof smart contract to utilize a verification key to verify correctness of the proof;

a database (165) arranged to operably store the target data and

a web server (167), coupled with the communication circuit (161), the block chain computing circuit (163), and the database (165), and arranged to operably acquire a read token transferred from the block chain system (180) through the communication circuit (161) or the block chain computing circuit (163) when the block chain system (180) determines an authorization token corresponding to an authorization token identification data as active;

wherein the communication circuit (161) is further arranged to operably receive a verification success notification transmitted from the block chain system (180) when the proof is determined as correct by the block chain system (180);

wherein the web server (167) is further arranged to operably transmit the sensitive data request to the data source system (150) through the communication circuit (161) after acquiring the read token, and to operably transfer the read token to the data source system (150) through the communication circuit (161) or the block chain computing circuit (163);

wherein if the read token transferred from the data service system (160) to the data source system (150) is valid, the web server (167) operably receives a sensitive data corresponding to the target data transmitted from the data source system (150) through

the communication circuit (161), and operably transmits the sensitive data to the data requester device (130) to the communication circuit (161).

15. The data service system (160) of claim 14, wherein the web server (167) is further arranged to operably transmit the authorization token identification data to the block chain system (180) after the sensitive data request transmitted from the data requester device (130) is received by the communication circuit (161).

16. The data service system (160) of claim 15, wherein the block chain system (180) is further arranged to operably execute an authorization policy smart contract to inspect whether the data service system (160) matches a predetermined authorization policy configured by the target user after receiving the authorization token identification data transmitted from the data service system (160).

17. The data service system (160) of claim 16, wherein the web server (167) acquires the read token transferred from the block chain system (180) through the communication circuit (161) or the block chain computing circuit (163) only if the block chain system (180) determines that the authorization token is active and the data service system (160) matches the predetermined authorization policy.

18. The data service system (160) of claim 15, wherein the web server (167) is further arranged to operably generate a data read request corresponding to a target requester and transmit the data read request to the data owner device (110) through the communication circuit (161) after the sensitive data request transmitted from the data requester device (130) is received by the communication circuit (161), and the web server (167) transmits the authorization token identification data to the block chain system (180) through the communication circuit (161) or the block chain computing circuit (163) only if the data read request is accepted by the target user.

19. The data service system (160) of claim 18, wherein the data owner device (110) further inquires the target user whether to accept the data read request, and the communication circuit (161) receives the authorization token identification data transmitted from the data owner device (110) only if the data read request is accepted by the target user.

20. The data service system (160) of claim 15, wherein the data source system (150) is further arranged to operably transfer the read token to the block chain system (180) after acquiring the read token;

wherein the block chain system (180) is further arranged to operably verify an activity of the read token after acquiring the read token, and to operably generate and transmit a verification success notice to the data source system (150) when determining the read token as active;

wherein after the verification success notice is received by the data source system (150), the communication circuit (161) receives the sensitive data corresponding to the target data transmitted from the data source system (150).