

**MATCHING-SERVICE SYSTEM AND MATCHING-SERVICE METHOD,
AGENCY SERVICE METHOD, AMOUNT MEASUREMENT METHOD AND
ACCOUNT MANAGEMENT DEVICE**

BACKGROUND

Technology Field

[0001] The present invention relates to a matching-service system and a matching-service method, and in particular, to a matching-service system and a matching-service method based on blockchain.

Description of Related Art

[0002] Nowadays, the matching services are implemented in the Internet to match the matching seekers and the matching provider in different locations. The matching-service provider provides a server, which is connected to the computer platforms of the matching seekers and the matching providers, and then provides a matching-service user interface to the matching seekers and the matching providers, so that the matching seekers and the matching providers can operate the matching-service user interface to obtain the desired matching results. Accordingly, the matching seekers and the matching providers can use the matching services provided by matching-service provider through the Internet without being restricted by the physical distance.

[0003] In general, the matching provider, which is qualified by the matching-service provider, can edit the goods or service information (including the matching conditions) through the matching-service user interface, and then the edited goods or service information can be upload to the server and stored in the database.

However, an existing problem is: after the matching seeker and the matching provider are matched through the matching-service system, if the matching provider revises the goods or service information thereof and saves the revision in the database through the matching-service user interface, such revision in the goods or service information may harm the rights of the other party (i.e. the matching seeker). On the other hand, if the right of the matching provider to revise the goods or service information is limited, it will make the matching-service platform inconvenient to use, thereby reducing the user's preference and willingness to use the matching-service platform.

SUMMARY

[0004] Therefore, this invention provides a matching-service system and a matching-service method that can allow the matching providers to revise the goods or service information without limitation and also protect the rights of matching seekers.

[0005] This invention provides a matching-service system, which comprises a user interface and a matching smart contract. The user interface is configured for displaying goods or service information to be matched, and issuing a message associated with a matching service to a smart contract execution unit according to an operation by a user. The smart contract execution unit issues a corresponding smart contract execution instruction according to the message associated with the matching service. The matching smart contract is deployed at a first address of a blockchain. The matching smart contract receives the smart contract execution instruction from the smart contract execution unit and executes functions defined in the matching smart contract according to the smart contract execution instruction. After the user operates the user interface to confirm a matching success, the user interface issues a matching-confirmation message to the smart contract execution unit, the smart contract execution unit issues a matching execution instruction to the matching smart

contract according to the matching-confirmation message, and the matching smart contract creates a storage zone at the first address of the blockchain according to the matching execution instruction and stores the current goods or service information or associated data thereof upon confirming the matching success in the storage zone.

[0006] In one embodiment, the smart contract execution unit is implemented by at least one of: a user front-end platform installed with the user interface and comprising a smart contract executing module, wherein the user interface issues the message associated with the matching service to the smart contract execution module according to the operation by the user, and the smart contract execution module issues a corresponding smart contract execution instruction to the matching smart contract according to the message associated with the matching service; and a server configured to issue the corresponding smart contract execution instruction to the matching smart contract according to the message associated with the matching service received from the user interface.

[0007] In one embodiment, the associated data of the goods or service information comprises at least one of: a compressed file according to the goods or service information; a hash value calculated by a hash algorithm according to the goods or service information, wherein the smart contract execution unit or the matching smart contract executes the hash algorithm to obtain the hash value; and a matching result message comprising consecutive related information after the matching success.

[0008] In one embodiment, the matching-service system further comprises a smart contract of mandate and authorization deployed at a second address of the blockchain or at an address of an additional blockchain, wherein the smart contract of mandate and authorization is configured to agree a mandate of the user and, when the user executes the matching smart contract, provide a function to pay a blockchain handling

fee as storing or changing information at the first address of the blockchain, and the additional blockchain uses a recording or accounting method for a blockchain transaction different from a recording or accounting method of the blockchain.

[0009] In one embodiment, the matching service is a strategy-matching service, the user is further classified to a strategy provider or a strategy seeker, and the strategy-matching service is configured to match the strategy provider who provides a strategy and the strategy seeker who interests in the provided strategy.

[0010] In one embodiment, the goods or service information stored at the first address of the blockchain comprises: a program code based on the strategy, wherein the program code is executed to reflect a buy or sell signal appeared in a finance market based on a content of the strategy to place an order through a brokerage platform, the smart contract execution unit reads the goods or service information or the associated data thereof stored at the first address of the blockchain to validate or proof the strategy, the brokerage platform provides a result for the order, and the matching smart contract calculates a performance and then stores the performance to the first address of the blockchain.

[0011] In one embodiment, a plurality of matching smart contracts are deployed at different addresses of the blockchain and correspond to a plurality of strategies provided by the strategy provider; or the blockchain is deployed with the matching smart contract only at the first address, a plurality of storage zones are created at the first address, and the storage zones at the first address deployed with the strategy smart contract are corresponding to a plurality of the strategies provided by the strategy provider.

[0012] The invention further provides a matching-service method, comprising: deploying a matching smart contract at a first address of a blockchain; and when a

matching-service user issues a matching request, the matching smart contract executes following functions of: creating a storage zone at the first address of the blockchain, and storing current goods and service information or associated data thereof as matching success in the storage zone.

[0013] The invention further provides an agency service method, comprising: deploying a smart contract of mandate and authorization at a first address of the blockchain based on a mandate and authorization of an agency service user; and when information is stored or changed at a second address of the blockchain or at an address of an additional blockchain based on a blockchain transaction requested by the agency service user, the smart contract of mandate and authorization executes following functions of: agreeing a mandate; confirming an authorization; executing a content of the mandate and authorization; and paying a blockchain handling fee as storing or changing the information at the first address of the blockchain or the address of the additional blockchain (without publishing the private key or private digital signature), wherein the additional blockchain uses a recording or accounting method for a blockchain transaction different from a recording or accounting method of the blockchain.

[0014] The invention further provides an amount measurement method, comprising: creating an account based on a user contract for a user, and deploying a currency token smart contract at an address of a blockchain, wherein the user contract defines a specific operation of the user for managing an account amount; creating a storage zone at the address of the blockchain; depositing an amount of a currency token, which is equal to an amount paid by the user based on the user contract, to the storage zone. According to the operation of the user for managing the account amount based on a content of the user contract, the currency token smart contract executes a

function of: measuring the remained amount of the account by the currency token, wherein the currency token is exchanged to cash by way of trust.

[0015] The invention further provides an account management device, comprising: an account flow management unit provided for a user to manage an account, so as to deposit, withdraw, or transfer money from the account of the user according to a flow management operation of the user; a flow amount measurement unit for issuing an amount measurement execution instruction to a currency token smart contract deployed at an address of a blockchain according to an amount measurement operation of the user, wherein the currency token smart contract executes, based on the amount measurement execution instruction, a function of: measuring a remained amount in an account of the user by a currency token, wherein an amount represented by the currency token is stored in a storage zone of the address of the blockchain; and an application exchange interface for receiving the amount returned by the flow amount measurement unit according to an exchange operation of the user, and exchanging the amount of the currency token smart contract with an equivalent cash of a designated account.

[0016] In one embodiment, the designated account is a cash account, and the exchange operation further comprises to deposit cash or to withdraw cash. When the exchange operation is to deposit cash, the application exchange interface deposits cash to the designated account based on an operation of the user, notifies a business end, and after finishing cash deposition, sends a deposition success message to the business end and executes following functions of a currency token smart contract at the address of the blockchain: recording and minting/increasing an equivalent amount of currency tokens in the storage zone of the user in the currency token smart contract; and when the exchange operation is to withdraw cash, the application exchange

interface executes a function of the currency token smart contract at the address of the blockchain based on the operation of the user: recording and burning/decreasing an equivalent amount of currency tokens in the storage zone of the user in the currency token smart contract; after burning the equivalent amount of currency tokens, the application exchange interface sends a withdrawal success message to the business end, transfers cash from the designated account to the account of the user, and then sends a cash transfer success message to the business end.

[0017] In one embodiment, a smart contract of mandate and authorization is deployed at a second address of the blockchain or at an address of an additional blockchain, the smart contract of mandate and authorization is configured to agree a mandate of a user, confirm an authorization, and when the user executes the currency token smart contract, provide a function to pay a blockchain handling fee as storing or changing information at the first address of the blockchain, and the additional blockchain uses a recording or accounting method for a blockchain transaction different from a recording or accounting method of the blockchain.

[0018] Therefore, the matching-service system and method of this invention can store the current goods or service information or associated data thereof upon confirming the matching success in the storage zone at an address of the blockchain, and the stored goods or service information or associated data thereof can be retrieved for comparison later. Accordingly, one part of the users in the matching service (the matching provider) can revise the goods or service information without limitation. In addition, the right of the other part of the users in the matching service (the matching seeker) can be protected.

BRIEF DESCRIPTION OF THE DRAWINGS

[0019] The disclosure will become more fully understood from the detailed

description and accompanying drawings, which are given for illustration only, and thus are not limitative of the present disclosure, and wherein:

[0020] FIG. 1a is a schematic diagram showing a matching-service system 10 according to an embodiment of this invention;

[0021] FIG. 1b is a schematic diagram showing a matching-service system 11 according to an embodiment of this invention;

[0022] FIG. 2 is a schematic diagram showing an agency service system 20 according to an embodiment of this invention;

[0023] FIG. 3 is a flow chart showing the step of mandating and authorizing to pay the handling fee of blockchain transaction according to an embodiment of this invention;

[0024] FIG. 4 is a flow chart showing a matching-service method according to an embodiment of this invention;

[0025] FIG. 5 is a flow chart showing an agency service method according to an embodiment of this invention;

[0026] FIG. 6 is a flow chart showing an amount measurement method according to an embodiment of this invention; and

[0027] FIG. 7 is a schematic diagram showing an account management device 70 according to an embodiment of this invention.

DETAILED DESCRIPTION OF THE DISCLOSURE

[0028] The present disclosure will be apparent from the following detailed description, which proceeds with reference to the accompanying drawings, wherein the same references relate to the same elements.

[0029] FIG. 1a is a schematic diagram showing a matching-service system 10 according to an embodiment of this invention. Referring to FIG. 1a, in one embodiment of this invention, the matching-service system 10 is constructed by a matching-service provider, and comprises a user interface 101, a smart contract execution unit 103, and a matching smart contract 105, which is deployed at an address 107 of the blockchain.

[0030] In one embodiment of this invention, the matching-service system 10 can be provided for multiple users. In an aspect of this embodiment, the users of the matching-service system 10 can be classified into two types of users, including the matching providers A and the matching seekers B. To be noted, either the matching providers A or the matching seekers B comprise one or more users. To make the description more comprehensive, they are described by A (the matching provider) and B (the matching seeker) only.

[0031] In one embodiment of this invention, the matching service can be, for example, a job matching service, a marriage matching service, a sell/buy matching service, or a strategy matching service for financial transaction, but this invention is not limited thereto.

[0032] In one embodiment of this invention, the user interface (UI) 101 is used to display the goods or service information to be matched. The users A and B of the matching services can decide what operations to perform according to the displayed goods or service information. For example, the matching provider A can operate the user interface 101 to store the "matching lure" in, for example, the cloud (e.g. a server). Here, the "matching lure" refers to the marketing content provided by the matching provider A for attracting the matching seeker B. On the other hand, the matching seeker B can also operate the user interface 101 to request the "matching

lure" of each matching provider A, and seek matching opportunities therefrom. In another example, for example, in the matching service of placing order or investment strategy, the matching provider A can operate the user interface 101 to upload the "goods or service information" of his placing order or investment strategy in the cloud. After the matching is successful, the matching seeker B can perform investment according to this strategy.

[0033] To be noted, the "goods or service information" to be matched is needed during or after the matching process of the matching provider A and the matching seeker B. However, the content of the "goods or service information" is related to the type of the matching service. In other words, different types of matching services correspond to different types of "goods or service information". Accordingly, no specific definition is made for the "goods or service information" here.

[0034] In one embodiment of this invention, the matching-service provider can deploy a matching smart contract 105 at the address 107 of the blockchain through the blockchain transaction. Once the matching of the matching seeker B and the matching provider A successes, the user interface 101 will issue a message associated to the matching service to the smart contract execution unit 103 according to the operation of the users A and B. For example, the message can be a matching success message. Afterwards, the smart contract execution unit 103 can issue a corresponding execution instruction to the matching smart contract 105 deployed at the address 107 of the blockchain according to the message associated to the matching service, and the matching smart contract 105 executes the function written or defined on the matching smart contract 105 according to the smart contract execution instruction.

[0035] For example, when the user A or B operates the user interface 101 to confirm the matching, the smart contract execution unit 103 can receive the matching success message. Then, the smart contract execution unit 103 will issue a matching execution instruction to the matching smart contract 105. Next, the matching smart contract 105 will create a storage zone at the address 107 of the blockchain based on the matching execution instruction, and store the current “goods or service information” or associated data thereof upon matching success in the storage zone. Accordingly, the content of the “goods or service information” can be retrieved for comparison later to check whether it has been changed or not. In one example of this embodiment, if the matching seeker B discovers that the goods or service information has been revised after the matching success, the matching seeker B can consider to continue the consecutive actions of the matching or to cancel the matching deal.

[0036] In one embodiment of this embodiment, the matching smart contract 105 can deploy the current “goods or service information” or “the associated data of the goods or service information” upon matching success in the storage zone at the address 107 of the blockchain for data storage by the blockchain transaction method.

[0037] The technical term "blockchain" used above refers to a "distributed" or "decentralized" data computing and storage platform architecture. Specifically, unlike the traditional transaction process, which must be conducted through a central platform, the "blockchain" includes several computer platforms, and the computer platforms are connected in a peer-to-peer manner for calculation and storage. Accordingly, due to the decentralization of the blockchain, the data stored in the blockchain cannot be tampered by attacking only one of the platforms, so the blockchain has the advantage of being immutable. In addition, the system

architecture of the blockchain is open, and the users can access the blockchain through a public interface.

[0038] In addition, the user can store the information to the blockchain by the blockchain transaction or deploying method, which is a common technical means in the blockchain application, so the detailed description thereof will be omitted.

[0039] To be noted, the technical term "smart contract" used in the present invention does not refer to a traditional contract with a counterparty. The so-called "smart contract" refers to a function pre-defined for a specific event stored at an address of the blockchain, and the function is executed according to an instruction. In brief, the so-called "smart contract" can be understood as a program code stored at an address of the blockchain, which can reflect a specific instruction to perform a corresponding function or calculation/operation.

[0040] In one embodiment of this invention, the programming language for coding the smart contract can include, for example, solidity, serpent, LLL, EtherScript, Sidechain, etc. However, the present invention is not limited thereto, and this invention does not exclude any new or other programming languages for coding the smart contract.

[0041] Furthermore, the deployed matching smart contract 105 of this embodiment can be coded to provide the following functions: creating a storage zone (not shown) at the first address 107 of the blockchain according to the matching execution instruction and storing the current goods or service information or associated data thereof upon matching success in the storage zone.

[0042] In one embodiment of this invention, the associated data of the goods or service information can be a compressed file according to the goods or service

information for obtaining more efficient data storage. Another implementation method thereof is to use the hash algorithm to calculate the corresponding hash value based on the content of the current "goods or service information" upon matching success. In the future, it is possible to compare the hash value to check whether the content of the "goods or service information" has been revised or not.

[0043] To be noted, the blockchain can serve not only as a ledger but also a notebook. In other words, the information recorded in this notebook (blockchain) can be used to validate or prove the future service without any change or update.

[0044] Furthermore, in the example of storing the hash values calculated based on the goods or service information, the matching smart contract 105 deployed at the address 107 of the blockchain can take the current goods or service information of the matching provider A upon matching success as an input, and calculate it with the hash algorithm, thereby obtaining the hash value corresponding to the goods or service information for matching and storing it in the storage zone at the address 107 of the blockchain. To be noted, since any computer-type platform can be used to calculate the hash value, the hash value can also be calculated by the smart contract execution unit 103, for example.

[0045] In one embodiment of this invention, the above hash algorithm can be HAVAL, MD2, MD4, MD5, PANAMA, RadioGatún, RIPEMD, RIPEMD-128/256, RIPEMD-160/320, SHA-0, SHA-1, SHA-2, SHA-256/224, SHA-512/384, SHA-3, etc. However, the aforementioned hash algorithms are only for illustrations, and the hash functions/algorithms of the present invention are not limited thereto. The present invention does not exclude any new or other algorithms for comparison, and algorithms with similar functions are also within the scope of the present invention.

[0046] In addition, the above-mentioned "hash value" is to input a variable length

of information (e.g. the goods or service information of the present invention) into the "hash function" to calculate a fixed-length hash value for outputting by a hash algorithm. The advantage of inputting the goods or service information into the hash function to calculate the hash value is that as long as the goods or service information changes slightly, the calculated hash value will be different. Therefore, for example, the goods or service information can be accessed at any time after matching success, and compare the hash value calculated based on the currently accessed goods or service information with the hash value stored upon matching success. According to the comparing result, it is easy to figure out whether the currently accessed goods or service information is consistent with the goods or service information upon matching success, or whether it has been revised, edited or changed.

[0047] Particularly, since the goods or service information or the associated data thereof (e.g. hash value) stored upon matching success is not an editable or revisable object by the users, once the matching is completed, the goods or service information or the associated data thereof upon matching success can be always stored in a specific storage zone at one address of the blockchain, and can be deleted unless necessary (e.g. cancel matching). Due to the immutable property of the blockchain, the users of the matching-service system can reliably compare the data to check whether the goods or service information has been revised or not after matching success.

[0048] The further implement of the smart contract execution unit 103 will be described hereinafter with reference to related drawings. FIG. 1b is a schematic diagram showing a matching-service system 11 according to an embodiment of this invention. As shown in FIG. 1b, in one embodiment of this invention, the matching-service system 11 established by the matching-service provider includes a

database 109, a matching smart contract 105 deployed at the address 107 of the blockchain, and a smart contract execution unit 103. In this embodiment, the smart contract execution unit 103 can be implemented by any of the user front-end platforms 103a and 103b, and the server 103c, which are installed with the user interface 101.

[0049] In this embodiment, the smart contract execution unit 103 is implemented by any of the user front-end platforms 103a and 103b, the user front-end platforms 103a and 103b can be computer platforms installed with the user interface 101 for providing the matching service. The user front-end platforms 103a and 103b can comprise, for example, a smart contract execution module (not shown). When the matching-service user A or B operates the user interface 101 to select a matching service (e.g. deciding to match), the user interface 101 can issue a message associated with the matching service (e.g. a matching success message) to the smart contract execution module according to the operation of the user A or B. Afterwards, the smart contract execution module can issue a corresponding smart contract execution instruction (e.g. a matching execution instruction) according to the message associated with the matching service to the matching smart contract 105.

[0050] In one embodiment of this invention, the computer platform used as the user front-end platform 103a or 103b can be, for example, a host computer, a notebook computer, a tablet computer, a PDA (personal digital assistant), a netbook, a smart phone, etc. However, the user front-end platforms 103a and 103b of the present invention are not limited to the above-mentioned computer platforms. Any computer device that can be installed with the user interface 101 of the matching service can be used as the user front-end platforms 103a and 103b.

[0051] In one embodiment of this invention, the smart contract execution module

can be loaded on the user front-end platforms 103a and 103b by installing the corresponding application software, and the smart contract execution module can have a dedicated user interface, or be the user interface 101 embedded in the matching service, so that the user can operate the smart contract execution module through the user interface 101 of the matching service. To be noted, the present invention is not limited thereto.

[0052] In the embodiment that implements the smart contract execution unit 103 by the server 103c, the server 103c is configured to issue a corresponding smart contract execution instruction to the matching smart contract 105 based on the message associated with the matching service outputted from the user interface 101. Specifically, when the matching-service user A or B operates the user interface 101 to select a matching service (e.g. deciding to match), the user interface 101 will issue a message associated with a matching service (e.g. a matching-confirmation message) to the server 103c based on the operation of the user A or B through the user front-end platform 103a or 103b. Afterwards, the server 103c can issue a corresponding smart contract execution instruction (e.g. a matching execution instruction) based on the message associated with the matching service.

[0053] In addition, in one embodiment of this invention, the server 103c can provide further functions other than the smart contract execution unit 103, such as the function of storing the non-published data in the database 109 through the server 103c. For example, the matching provider A and the matching seeker B can operate the matching-service user interface 101 loaded on the user front-end platforms 103a and 103b to register an account (become a registered member), and the registered member data can be stored in the database 109 through the server 103c. In addition, the server 103c can also store the data associated with “the goods or service information”

and/or “the matching lure” before the matching step. Moreover, the server 103c can further perform a hash calculation with “the goods or service information” upon matching success and then store it in a storage zone at an address of the blockchain through the matching smart contract 105. To be noted, the data that can be processed by the server 103c in this invention is not limited thereto.

[0054] It should be noted that a general server (e.g. the server 103c of the embodiment shown in FIG. 1b) can be a computer device, which may include a processor, a memory, an input/output interface, a communication interface, and a bus. The processor, memory, input/output interface, and communication interface are internally coupled or communicated through the bus. Accordingly, the server 103c of the above-mentioned embodiment can be carried out by the hardware of the above-mentioned computer device cooperated with the software and/or firmware to achieve the function of "configured to issue a corresponding smart contract execution instruction to the matching smart contract 105 based on the message associated with the matching service outputted from the user interface 101". The technical art of achieving the above-mentioned configuration can be easily understood by those with ordinary knowledge in the art through the enlightenment of the description of the above-mentioned embodiment, so it will not be described in detail here.

[0055] In order to understand the above-mentioned embodiment of the present invention more specifically, since the blockchain is often used in the financial field, the following will take the "strategy matching service" for investment as an example of the "matching service" for further explanation. Generally speaking, the common strategy matching platforms allow the strategy providers to provide "investment strategies", and the strategy seekers who are interested in the investment strategy can match the strategy provided by the strategy provider and invest according to the

investment strategy. That is, in this embodiment, the matching provider is in the role of the strategy provider, and the matching seeker is in the role of the strategy seeker.

[0056] With reference to FIG. 1b, in the embodiment of strategy matching service, the strategy matching-service provider will provide a strategy matching-service system (e.g. the matching-service system 11 as shown in FIG. 1b). In the matching-service system 11, the strategy provider A (i.e. the matching provider A) and the strategy seeker B (i.e. the matching seeker B), which is seeking for the strategy matching can individually operate the matching-service user interface 101 loaded on the user front-end platforms 103a and 103b to register as a registered member, and the registered member data can be stored in the database 109 through the server 103c.

[0057] In addition, the strategy provider A can operate the matching-service user interface 101 loaded on the user front-end platform 103a to store the investment strategy for matching and the “matching lure” to the database 109 through the server 103c. To be noted, the “matching lure” can be, for example, the rate of return (e.g. +30%) obtained by investing in accordance with this investment strategy during the past period of time (e.g. the past 6 months). The investor seeking the strategy matching (the strategy seeker B) can find the above-mentioned "matching lure" of the investment strategy through the matching-service user interface 101 of the user front-end platform 103b. If the investor determines that the provided rate of return is acceptable, the strategy seeker B who seeks for strategy matching can operate the matching-service user interface 101 of the user front-end platform 103b to match the investment strategy provided by the strategy provider A.

[0058] In this embodiment of the invention, the address 107 of the blockchain can be further deployed with the matching smart contract 105. Once the strategy seeker B and the strategy provider A are successfully matched, the smart contract execution

unit 103 can issue a matching execution instruction according to the matching success message outputted from the user interface 101, and the matching smart contract 105 can store the goods or service information or associated data thereof in the storage zone at the address 107 of the blockchain created by the matching smart contract 105 based on the matching execution instruction. For example, in the case of storing the goods or service information, the strategy to be matched with the strategy seeker B and other important information for matching can be stored in the storage zone at the address 107 of the blockchain. In the case of storing the associated data of the goods or service information, a compressed file or a calculated hash value including the strategy to be matched with the strategy seeker B and other important information for matching can be stored in the storage zone at the address 107 of the blockchain, and any revision or change is not allowed.

[0059] To be noted, in one embodiment of this invention, if the provided strategy is in a text format, the goods or service information can comprise the investment strategy in text. In one embodiment of this invention, the goods or service information, which is stored in the storage zone at the address 107 of the blockchain by the strategy provider A through operating the matching-service user interface 101, can comprise the program code that is coded based on the strategy. In this case, even the strategy seeker B can access the goods or service information after matching success, the strategy seeker B may be not able to realize the entire investment strategy from the program code. However, since the current goods or service information or associated data thereof (e.g. the compressed file or hash value) upon matching success is stored in the storage zone at an address of the blockchain, and it is possible to check whether the strategy has been revised or changed anytime in the future by comparing the stored goods or service information upon matching success with the current goods

or service information at the check point. This configuration can protect the rights and interests of strategy seeker B after matching success.

[0060] In one embodiment of this invention, after matching success, for example, a strategy execution platform (not shown) can be used to react to the buy or sell signal appeared in the financial market and execute the program code written according to the strategy. Although the general user cannot identify whether the program code has been changed or not, the strategy can be verified by the smart contract execution unit 103 after reading the goods or service information or the associated data thereof stored in the storage zone at the address 107 of the blockchain. Furthermore, the "associated data of the goods or service information" may also include matching result information. For example, the matching-service provider can cooperate with a brokerage firm. If the investment strategy is "When the stock market falls by 5%, then buy in.", when receiving a buy or sell signal indicating that the stock market falls by 5%, it will notify the brokerage firm and entrust the brokerage firm to place an order through the brokerage platform. Then, the brokerage platform will report the result of the order, and the performance will be stored in the storage zone at the address 107 of the blockchain after calculating the performance. Afterwards, the user can operate the user interface 101 to access the blockchain for realizing the performance. Herein, the performance is an example of a matching result message. To be noted, the above-mentioned investment strategy is only an example, and the actual investment strategies can be more complicated. For the sake of brevity, it is not described in detail here.

[0061] In one embodiment of this invention, the number of the strategies provided by one strategy provider is not limited to one. In other words, one strategy provider can provide multiple investment strategies. In this embodiment, a plurality of

matching smart contracts 105 can be deployed at different addresses of the blockchain and are corresponding to a plurality of strategies provided by the strategy provider. Alternatively, one matching smart contract 105 is deployed at an address of the blockchain, and a plurality of storage zones are created at the address. The multiple storage zones at the address of the matching smart contract 105 are corresponding to a plurality of strategies provided by the strategy provider. This aspect can be achieved by properly coding the program code of the smart contract, and this invention is not limited. In addition, one strategy seeker can match a plurality of investment strategies, and this invention is not limited.

[0062] In general, the blockchain external transaction in the blockchain mechanism must be charged by “a blockchain transaction handling fee” or “gas”. In addition, different types of blockchains (the blockchains using different recording or accounting methods) may charge different types of virtual currencies for the blockchain handling fee. For example, in an Ethereum, the blockchain transaction service must be paid by Ether. In the embodiment of this invention, the common blockchain types (virtual currencies) comprise bitcoin, Ether, Ripple, Litecoin, etc., and this invention is not limited thereto.

[0063] However, when the user performs the operations related to blockchain, it is a more convenient way to entrust a matching-service provider to pay the blockchain handling fees. Therefore, in the embodiment of the present invention, if the matching-service user mandates and authorizes the matching-service provider to handle the blockchain transaction handling fee generated corresponding to each blockchain external transaction, the matching-service system and method of this invention can be more useful.

[0064] FIG. 2 is a schematic diagram showing an agency service system 20

according to an embodiment of this invention, which is used to pay the blockchain transaction handling fee generated corresponding to the blockchain transaction on behalf of the matching-service user. Referring to FIG. 2, the agency service system 20 comprises a user interface 101, a smart contract execution unit 103, a smart contract 205 of mandate and authorization deployed at the first address 107-1 of the blockchain. When the user A or B operates the user interface 101 to perform a blockchain external transaction of the blockchain (e.g. the user A or B intends to store or revise the information stored at the address 107-2 of the blockchain, such as the matching smart contract 105 of the embodiments shown in FIGS. 1a and 1b), the user interface 101 can issue an entrust-to-pay instruction based on the operation of the user A or B to request the smart contract execution unit 103 to execute the function of the smart contract 205 of mandate and authorization stored at the first address 107-1 of the blockchain to implement the function of paying the blockchain handling fee required for saving or revising the information stored at the second address 107-2 of the blockchain. In one embodiment of this invention, the smart contract 205 of mandate and authorization can be deployed at an address of an additional blockchain other than the blockchain deployed with the matching smart contract 105. In this case, the blockchain deployed with the smart contract 205 of mandate and authorization uses a recording or accounting method for the blockchain transaction different from a recording or accounting method used by the blockchain deployed with the matching smart contract 105. For example, the blockchain deployed with the matching smart contract 105 uses “bitcoin” as the means for recording or accounting, but the blockchain deployed with the smart contract 205 of mandate and authorization uses “Litecoin” as the means for recording or accounting. When the smart contract 205 of mandate and authorization pays the blockchain handling fee to the matching smart contract 105 deployed in a different blockchain, a “virtual

currency exchange interface” is introduced. To be noted, the “virtual currency exchange interface” can be easily understood by those with ordinary knowledge in the art through the enlightenment of the description of the above-mentioned embodiment, so it will not be described in detail here.

[0065] It should be noted, the function of paying blockchain handling fees of the above-mentioned smart contract 205 of mandate and authorization deployed at the first address 107-1 of the blockchain can be replaced by a third-party payment platform (not shown). For example, the third-party payment platform can be a traditional centralized payment platform. Compared with the conventional art, to pay the blockchain transaction handling fee through the blockchain has the advantages of open and immutability.

[0066] An example of an agency operation for paying the blockchain handling fee of the blockchain transaction of an assignor will be described in the following example with reference to FIGS. 2 and 3. FIG. 3 is a flow chart showing the step of mandating and authorizing to pay the handling fee of blockchain transaction according to an embodiment of this invention. First, when the user A or B operates the user interface 101 to store or revise the information stored at an address of the blockchain (e.g. an address 107-2 of the same blockchain or an additional blockchain), the user A or B will be defined as the assigner for paying the blockchain handling fee and issue a mandate request through the user interface 101 (step S31). Next, the smart contract execution unit 103 issues a mandate instruction to a smart contract 205 of mandate and authorization deployed at an address 107-1 of the blockchain (step S32), and then the smart contract 205 of mandate and authorization deployed at an address 107-1 of the blockchain receives the mandate instruction (step S33). Based on the mandate instruction, the smart contract 205 of mandate and authorization can

hash or unify the mandate content from the assignor, wherein the mandate content comprises, for example, the address of the smart contract in this mandate request, the identity of the assignor (e.g. the address of the assignor in the blockchain, the public key generated based on the address, etc.), the function and parameters of the smart contract to be executed, etc. (step S34). As mentioned above, if the mandate item is to execute the smart contract deployed at another address of the same blockchain or an additional blockchain (e.g. the smart contract at the address 107-2 of the blockchain in the embodiment of FIG. 2), the execution instruction address information thereof will be included in the mandate content. In the step S32, while issuing the mandate instruction to the smart contract 205 of mandate and authorization, the smart contract execution unit 103 also issues an “authorization request” (or “delegated power request”) to request the assignor to authorize (or delegate) the mandate thereof (step S35). Afterwards, the address of the assignor in the blockchain (i.e. the wallet of the assignor) receives the authorization request and the authorization content from the smart contract execution unit 103 (step S36). Then, the assignor can hash/unify and sign the authorization content (step S37), and the signed authorization content is sent back to the smart contract execution unit 103 (step S38). According to the returned signed authorization content, the smart contract execution unit 103 will issue a mandate authorization comparing instruction (step S39). After the smart contract 205 of mandate and authorization receives the mandate authorization comparing instruction (step S40), the smart contract 205 of mandate and authorization will compare the mandate content received in step S33 with the authorization content received in step S40 so as to verify and validate/proof whether the assignor and the mandate content are identical to the authorizer and the authorization content. It is also possible to compare the assignor’s address received in step S33 with the public assignor’s address, or to compare the public key generated

based on the assignor's address obtained from the signed authorization content with the public assignor's address (step S41). If the comparison result indicates that the mandate content is identical to the authorization content, or the assignor's address or the public key is identical, the blockchain address and execution instruction will be obtained from the mandate/authorization content, and then the mandate/authorization content is executed as well as paying the blockchain handling fee as storing or changing information at the address of the same blockchain or the additional blockchain. For example, the address 107-2 of the same blockchain or the additional blockchain is obtained from the mandate/authorization content, the instruction to execute the smart contract (e.g. the matching smart contract 105 of FIGS. 1a and 1b) deployed thereon is also obtained from the mandate/authorization content, and the blockchain handling fee generated by executing the smart contract is paid upon executing the smart contract (step S42). If the comparison result indicates that the mandate content is not identical to the authorization content, or the identity of the assignor (the assignor's address or the public key) is not identical, the execution is halted (step S43).

[0067] FIG. 4 is a flow chart showing a matching-service method according to an embodiment of this invention. With reference to FIGS. 1a and 4, the matching-service method comprises the steps of: deploying a matching smart contract 105 at an address 107 of a blockchain (step S401); when a matching-service user A or B issues a matching request, sending a matching execution instruction to the matching smart contract 105 deployed at the address 107 of the blockchain (step S403); the matching smart contract 105 creates a storage zone at the address 107 of the blockchain according to the matching execution instruction (step S405); and the matching smart contract 105 stores the current goods and service information or

associated data thereof as matching success in the storage zone according to the matching execution instruction (step S407).

[0068] FIG. 5 is a flow chart showing an agency service method according to an embodiment of this invention. With reference to FIGS. 2 and 5, in the agency service method, a smart contract 205 of mandate and authorization is deployed at a first address 107-1 of the blockchain based on a mandate and authorization of the agency service user A or B (step S501). When the information is stored or changed at a second address 107-2 of the blockchain based on a blockchain transaction requested by the agency service user A or B, the agency service user A or B issues a mandate instruction to the smart contract 205 of mandate and authorization (step S503). Next, the smart contract 205 of mandate and authorization executes the following functions based on the mandate instruction: agreeing the mandate; confirming the authorization, executing a content of the mandate and authorization; and paying a blockchain handling fee as storing or changing the information at the second address 107-2 of the blockchain or an address of an additional blockchain (step S505). To be noted, in the step S505, the smart contract 205 of mandate and authorization deployed at the first address 107-1 of the blockchain can pay for the blockchain handling fee at the address of different blockchain. Herein, the “additional blockchain” or “different blockchain” uses a recording or accounting method for the blockchain transaction different from a recording or accounting method of the blockchain deployed with the smart contract 205 of mandate and authorization.

[0069] In one embodiment of this invention, in order to use the advantages of open and immutable of the blockchain, under the current laws and regulations, to calculate the cash flow generated in the account (e.g. the trust account agreed by the provider

and the client) based on the operation for a specific purpose, a currency token smart contract, which has a function of measuring currency amount by the currency token (e.g. a crypto token), can be deployed at an address of a blockchain. Herein, the cash flow generated based on the operation for a specific purpose can be, for example, the service fee generated as the matching-service user uses the matching service in the embodiment of FIG. 1a, or the returns generated in the investment of placing order by the brokerage platform according to the matched strategy, which is obtained from the strategy matching service. To be noted, this invention is not limited thereto. Accordingly, an account measurement method will be described hereinafter with reference to the drawing.

[0070] FIG. 6 is a flow chart showing an amount measurement method according to an embodiment of this invention. At first, an account is created based on a user contract for a user. For example, the account can be a trust property account established by a provider based on agency affairs. The user contract is an operation of the user to manage the account amount for a specific purpose, such as the amount management of service fee deduction for service purposes, the calculation management of investment returns for investment purposes, and to deploy a currency token smart contract at an address of the blockchain (step S601). Next, a storage zone is created at the address of the blockchain according to the blockchain operation of the user (step S603). Then, an amount of currency token, which is equal to an amount paid by the user based on the user contract, is deposited to the storage zone (step S605). Herein, the amount paid by the user based on the user contract is the account currency amount to be managed for the specific purpose, and the currency token (e.g. the crypto token) is used to replace the cash. Finally, according to the operation of the user for managing the account amount based on a content of the user

contract, an amount measurement instruction is issued to the currency token smart contract, and the currency token smart contract measures the remained amount of the account by the currency token according to the amount measurement instruction (step S607). In one embodiment of this invention, if the account to be managed is agreed as a trust account, the currency token can be exchanged to cash by way of trust, so that the user may retrieve the cash back.

[0071] This invention also provide a device that allows the user to operate the currency token smart contract to measure the currency amount and manage the account corresponding to the method of FIG. 6. FIG. 7 is a schematic diagram showing an account management device 70 according to an embodiment of this invention. As shown in FIG. 7, the account management device 70 comprises an account flow management unit 701, a flow amount measurement unit 703, and an application exchange interface 705.

[0072] In one embodiment of this invention, the account flow management unit 701 is provided for a user to manage an account. For example, when the user intends to perform the operation of deposition, withdraw, or transfer, the account flow management unit 701 can deposit, withdraw, or transfer money from the account of the user according to a flow management operation of the user.

[0073] In one embodiment of this invention, the user can perform a function defined on a currency token smart contract (e.g. the currency token smart contract as shown in FIG. 6) deployed at an address of the blockchain through the flow amount measurement unit 703. In more detailed, the flow amount measurement unit 703 can issue an amount measurement execution instruction to the currency token smart contract deployed at the address of the blockchain according to an amount measurement operation of the user. Next, the currency token smart contract executes,

based on the amount measurement execution instruction, a function of: measuring a remained amount in an account of the user by a currency token, wherein an amount represented by the currency token is stored in a storage zone of the address of the blockchain. The storage zone is created through the currency token smart contract for executing the function of the currency token smart contract.

[0074] In one embodiment of this invention, the user can perform the exchange operation of currency token and cash through the application exchange interface 705. Specifically, according to the exchange operation of the user, the application exchange interface 705 receives the amount returned by the flow amount measurement unit 703, and exchanges the amount of the currency token smart contract with an equivalent cash of a designated account.

[0075] In one embodiment of this invention, the exchange operation further comprises a step of depositing cash. When the user performs an exchange operation to deposit cash, the application exchange interface 705 deposits cash to the designated account based on an operation of the user, and notifies a business end. Next, after finishing the cash deposition, the application exchange interface 705 sends a deposition success message to the business end and issues a currency token minting instruction to the currency token smart contract deployed at the address of the blockchain. Accordingly, the currency token smart contract can record and mint/increase an equivalent amount of currency tokens in the storage zone of the user in the currency token smart contract based on the currency token minting instruction.

[0076] In one embodiment of this invention, the exchange operation further comprises a step of withdrawing cash. When the exchange operation is to withdraw cash, the application exchange interface 705 issues a currency token burning instruction to the currency token smart contract at the address of the blockchain based

on an operation of the user. According to the currency token burning instruction, the currency token smart contract records and burns/decreases an equivalent amount of currency tokens in the storage zone of the user in the currency token smart contract. After burning the equivalent amount of currency tokens, the application exchange interface sends a withdrawal success message to the business end, transfers cash from the designated account to the account of the user, and then sends a cash transfer success message to the business end.

[0077] In one embodiment of this invention, when executing the function of the above-mentioned currency token smart contract, it is possible to mandate the smart contract (e.g. the smart contract 205 of mandate and authorization of FIG. 2) deployed at an additional address of the same blockchain or at an address of an additional blockchain to pay the blockchain handling fee. Specifically, a smart contract of mandate and authorization is deployed at an additional address of the blockchain or at an address of an additional blockchain, and the smart contract of mandate and authorization is configured to agree a mandate of a user, confirm an authorization, and when the user executes the currency token smart contract, provide a function to pay a blockchain handling fee as storing or changing information at the address of the blockchain. As mentioned above, the additional blockchain uses a recording or accounting method for a blockchain transaction different from a recording or accounting method of the blockchain.

[0078] This invention combines the user account with the currency token smart contract, so that the amounts of all accounts can be publicized, and the capital account can only be increased or decreased based on the currency tokens. This feature is benefit to provide the user with a transparent and safe transaction environment. Moreover, the transfer of funds can only be done based on the currency tokens, and

the currency token transfer, and the currency token records the transfer information, so that this invention can also provide the money laundering prevention function.

[0079] To be noted, the various interfaces and/or units mentioned above can be achieved through, for example, a system-on-chip or a computer device. If the various interfaces and/or units are achieved by a computer device, the computer device at least includes a display, a processor, a memory, a user input/output (I/O) interface, a communication interface, and a bus, wherein the processor, the memory, the user input/output interface, and the communication interface are internally coupled or communicated through the bus. Specifically, the processor of the computer device can implement these interfaces and/or units by reading the program code in the memory in cooperation with the peripheral hardware components. The technical art of achieving the above-mentioned configuration can be easily understood by those with ordinary knowledge in the art through the enlightenment of the description of the above-mentioned embodiment, so it will not be described in detail here. In addition, in an embodiment of the present invention, the program code may be in the form of a computer program product, such as a package software installed on a desktop computer or a laptop computer, or may be an application (APP) installed on a mobile computing device. In addition, it is also possible to load the program code directly on a browser to form the above-mentioned unit or interface, and the present invention is not limited to the above.

[0080] Those with ordinary knowledge in the art should understand that the method provided by the embodiment of this invention can be implemented programmatically as program code or assembled and translated executable code, mechanical code, etc., and stored or temporarily stored in a computer-readable storage medium to provide a computer to execute the recorded program instructions. For example, the processor

of the computer reads the program code written according to the method from the storage medium into the memory (or temporarily stored on the storage medium) to implement the steps of the method in each embodiment of the present invention. However, the above-mentioned technology can be understood by those with ordinary knowledge in the art, and will not be further described here.

[0081] Although the disclosure has been described with reference to specific embodiments, this description is not meant to be construed in a limiting sense. Various modifications of the disclosed embodiments, as well as alternative embodiments, will be apparent to persons skilled in the art. It is, therefore, contemplated that the appended claims will cover all modifications that fall within the true scope of the disclosure.

CLAIMS

What is claimed is:

1. A matching-service system, comprising:
 - a user interface for displaying goods or service information to be matched, and issuing a message associated with a matching service to a smart contract execution unit according to an operation by a user, wherein the smart contract execution unit issues a corresponding smart contract execution instruction according to the message associated with the matching service; and
 - a matching smart contract deployed at a first address of a blockchain, wherein the matching smart contract receives the smart contract execution instruction from the smart contract execution unit and executes functions defined in the matching smart contract according to the smart contract execution instruction;wherein, after the user operates the user interface to confirm a matching success, the user interface issues a matching-confirmation message to the smart contract execution unit, the smart contract execution unit issues a matching execution instruction to the matching smart contract according to the matching-confirmation message, and the matching smart contract creates a storage zone at the first address of the blockchain according to the matching execution instruction and stores the current goods or service information or associated data thereof upon confirming the matching success in the storage zone.
2. The matching-service system of claim 1, wherein the smart contract execution

unit is implemented by at least one of:

a user front-end platform installed with the user interface and comprising a smart contract executing module, wherein the user interface issues the message associated with the matching service to the smart contract execution module according to the operation by the user, and the smart contract execution module issues a corresponding smart contract execution instruction to the matching smart contract according to the message associated with the matching service; and

a server configured to issue the corresponding smart contract execution instruction to the matching smart contract according to the message associated with the matching service received from the user interface.

3. The matching-service system of claim 1, wherein the associated data of the goods or service information comprises at least one of:

a compressed file according to the goods or service information;

a hash value calculated by a hash algorithm according to the goods or service information, wherein the smart contract execution unit or the matching smart contract executes the hash algorithm to obtain the hash value; and

a matching result message comprising consecutive related information after the matching success.

4. The matching-service system of claim 1, further comprising a smart contract of mandate and authorization deployed at a second address of the blockchain or at an address of an additional blockchain, wherein the smart contract of mandate and authorization is configured to agree a mandate of the user and, when the user executes the matching smart contract, provide a function to pay a blockchain

handling fee as storing or changing information at the first address of the blockchain, and the additional blockchain uses a recording or accounting method for a blockchain transaction different from a recording or accounting method of the blockchain.

5. The matching-service system of claim 1, wherein the matching service is a strategy-matching service, the user is further classified to a strategy provider or a strategy seeker, and the strategy-matching service is configured to match the strategy provider who provides a strategy and the strategy seeker who interests in the provided strategy.
6. The matching-service system of claim 5, wherein the goods or service information stored at the first address of the blockchain comprises: a program code based on the strategy, wherein the program code is executed to reflect a buy or sell signal appeared in a finance market based on a content of the strategy to place an order through a brokerage platform, the smart contract execution unit reads the goods or service information or the associated data thereof stored at the first address of the blockchain to validate or proof the strategy, the brokerage platform provides a result for the order, and the matching smart contract calculates a performance and then stores the performance to the first address of the blockchain.
7. The matching-service system of claim 5, wherein a plurality of the matching smart contracts are deployed at different addresses of the blockchain and correspond to a plurality of the strategies provided by the strategy provider; or the blockchain is deployed with the matching smart contract only at the first address, a plurality of storage zones are created at the first address, and the storage zones at the first address deployed with the strategy smart contract are

corresponding to a plurality of the strategies provided by the strategy provider.

8. A matching-service method, comprising:

deploying a matching smart contract at a first address of a blockchain; and

when a matching-service user issues a matching request, the matching smart contract executes following functions of: creating a storage zone at the first address of the blockchain, and storing current goods and service information or associated data thereof as matching success in the storage zone.

9. An agency service method, comprising:

deploying a smart contract of mandate and authorization at a first address of the blockchain based on a mandate and authorization of an agency service user; and

when information is stored or changed at a second address of the blockchain or at an address of an additional blockchain based on a blockchain transaction requested by the agency service user, the smart contract of mandate and authorization executes following functions of: agreeing a mandate; confirming an authorization; executing a content of the mandate and authorization; and paying a blockchain handling fee as storing or changing the information at the first address of the blockchain or the address of the additional blockchain, wherein the additional blockchain uses a recording or accounting method for a blockchain transaction different from a recording or accounting method of the blockchain.

10. An amount measurement method, comprising:

creating an account based on a user contract for a user, and deploying a currency token smart contract at an address of a blockchain, wherein the user contract

defines a specific operation of the user for managing an account amount;
creating a storage zone at the address of the blockchain;
depositing an amount of a currency token, which is equal to an amount paid by
the user based on the user contract, to the storage zone; and
according to the operation of the user for managing the account amount based
on a content of the user contract, the currency token smart contract executes
a function of: measuring the remained amount of the account by the currency
token, wherein the currency token is exchanged to cash by way of trust.

11. An account management device, comprising:

an account flow management unit provided for a user to manage an account, so
as to deposit, withdraw, or transfer money from the account of the user
according to a flow management operation of the user;
a flow amount measurement unit for issuing an amount measurement execution
instruction to a currency token smart contract deployed at an address of a
blockchain according to an amount measurement operation of the user,
wherein the currency token smart contract executes, based on the amount
measurement execution instruction, a function of: measuring a remained
amount in an account of the user by a currency token, wherein an amount
represented by the currency token is stored in a storage zone of the address
of the blockchain; and
an application exchange interface for receiving the amount returned by the flow
amount measurement unit according to an exchange operation of the user,
and exchanging the amount of the currency token smart contract with an
equivalent cash of a designated account.

12. The account management device of claim 11, wherein the designated account is a cash account, and the exchange operation further comprises to deposit cash or to withdraw cash:

when the exchange operation is to deposit cash, the application exchange interface deposits cash to the designated account based on an operation of the user, notifies a business end, and after finishing cash deposition, sends a deposition success message to the business end and executes following functions of a currency token smart contract at the address of the blockchain: recording and minting/increasing an equivalent amount of currency tokens in the storage zone of the user in the currency token smart contract; and

when the exchange operation is to withdraw cash, the application exchange interface executes a function of the currency token smart contract at the address of the blockchain based on the operation of the user: recording and burning/decreasing an equivalent amount of currency tokens in the storage zone of the user in the currency token smart contract; after burning the equivalent amount of currency tokens, the application exchange interface sends a withdrawal success message to the business end, transfers cash from the designated account to the account of the user, and then sends a cash transfer success message to the business end.

13. The account management device of claim 12, wherein a smart contract of mandate and authorization is deployed at a second address of the blockchain or at an address of an additional blockchain, the smart contract of mandate and authorization is configured to agree a mandate of a user and, when the user executes the currency token smart contract, provide a function to pay a blockchain handling fee as storing or changing information at the first address of

the blockchain, and the additional blockchain uses a recording or accounting method for a blockchain transaction different from a recording or accounting method of the blockchain.