

[DESCRIPTION]

[Invention Title]

METHOD FOR PROCESSING TRANSACTION VIA EXTERNAL NODE ON
BLOCKCHAIN AND APPARATUS FOR PERFORMING THE METHOD

5 [Technical Field]

The present invention relates to a method of processing a transaction through an external node on a blockchain and an apparatus for performing the method. More particularly, the present invention relates to a method and apparatus for allowing limited operation of an external node in a blockchain network by setting a
10 predetermined right in the external node.

[Background Art]

A blockchain may be a digital ledger on which information on transactions made in a public network or a private network is encrypted and shared among members of the corresponding network.

15 A copy of a transaction ledger is distributed to each network member, and thus every time a new transaction occurs, an authentication procedure for the corresponding transaction may proceed through agreement of members.

Blockchain-based transaction information cannot be arbitrarily changed. Therefore, the reliability of transactions is increased, and information tracking is easy.
20 Particularly, in the financial service field, the blockchain technology is being employed to increase work efficiency and construct a new service base.

Transparent transactions through a distributed ledger system allow a reduction in security, monitoring, and regulation costs. The blockchain technology can be applied not only to the financial field but also to logistics, distribution, and
25 even the government's public service.

In an existing public blockchain network, such as Bitcoin, participant nodes may operate with the same rights, whereas in a private blockchain network or a permissioned blockchain network, nodes may operate with differential rights.

Consequently, it is necessary to research a method for setting differential (or
5 limited) rights to operate in a blockchain.

[Disclosure]

[Technical Problem]

Objects of the present invention are to overcome all of the above-described problems.

10 The present invention is directed to allowing limited operation of an external node in a blockchain network by setting a predetermined right in the external node.

The present invention is also directed to hierarchically limiting an access right to a node by using channels, channel codes, data classifications, etc. in a blockchain network.

15 [Technical Solution]

Representative configurations of the present invention for achieving the above objects are as follows.

One aspect of the present invention provides a method of processing a transaction through an external node on a blockchain comprising setting, by a setup
20 node, internal nodes and external nodes, setting, by the setup node, a first data transaction right in the internal nodes and setting, by the setup node, a second data transaction right in the external nodes, wherein the first data transaction right is a right which is set in the internal nodes to operate in a blockchain network, and the second data transaction right is a right which is set in the external nodes to operate in
25 the blockchain network.

Another aspect of the present invention provides a setup node for processing a transaction through an external node on a blockchain comprising a communication unit implemented to communicate with an external node and a processor operatively connected to the communication unit, wherein the processor is implemented to set internal nodes and external nodes, set a first data transaction right in the internal nodes, and set a second data transaction right in the external nodes, wherein the first data transaction right is a right which is set in the internal nodes to operate in a blockchain network and the second data transaction right is a right which is set in the external nodes to operate in the blockchain network.

10 [Advantageous Effects]

According to the present invention, limited operation of an external node in a blockchain network is allowed by setting a predetermined right in the external node.

Further, according to the present invention, an access right to a node by using channels, channel codes, data classifications, etc is hierarchically limited in a blockchain network.

[Description of Drawings]

FIG. 1 is a conceptual diagram illustrating a method of processing a transaction through a node in a blockchain network according to an exemplary embodiment of the present invention.

20 FIG. 2 is a conceptual diagram illustrating a method of processing a transaction which is caused by an external node according to an exemplary embodiment of the present invention.

FIG. 3 is a conceptual diagram illustrating a method for setting a limited data transaction right in an external node according to an exemplary embodiment of the present invention.

FIG. 4 is a conceptual diagram illustrating a method for setting a limited data transaction right in an external node according to an exemplary embodiment of the present invention.

FIG. 5 is a conceptual diagram illustrating a method for setting a limited data transaction right in an external node according to an exemplary embodiment of the present invention.

FIG. 6 illustrates a method of hierarchically setting external nodes according to an exemplary embodiment of the present invention.

FIG. 7 is a conceptual diagram illustrating a method of trading assets through an external node according to an exemplary embodiment of the present invention.

[Modes of the Invention]

Detailed descriptions of the present invention will be made with reference to the accompanying drawings illustrating specific embodiments of the present invention as examples. These embodiments will be described in detail such that the present invention can be performed by those skilled in the art. It should be understood that various embodiments of the present invention are different but are not necessarily mutually exclusive. For example, a specific shape, structure, and characteristic of an embodiment described herein may be implemented in another embodiment without departing from the scope and spirit of the present invention. In addition, it should be understood that a position or an arrangement of each component in each disclosed embodiment may be changed without departing from the scope and spirit of the present invention. Accordingly, there is no intent to limit the present invention to detailed descriptions to be described below. The scope of the present invention is defined by the appended claims and encompasses all

equivalents that fall within the scope of the appended claims. Like numbers refer to equal or like functions throughout the description of the figures.

Hereinafter, in order for those skilled in the art to easily perform the present invention, exemplary embodiments of the present invention will be described in
5 detail with reference to the accompanying drawings.

An exemplary embodiment of the present invention provides a method of allowing limited access to a specific node in a blockchain network by setting node-specific rights in the blockchain network.

Digital asset-backed securities disclosed in the following exemplary
10 embodiments of the present invention may be digital securities which are issued on the basis of assets and tradable in a network such as a blockchain. Hereinafter, digital asset-backed securities will be indicated by the term “DABS,” and DABS may be interpreted in a broad sense as including various means which have a predetermined value and which are tradable in a network such as a blockchain.

15 FIG. 1 is a conceptual diagram illustrating a method of processing a transaction through a node in a blockchain network according to an exemplary embodiment of the present invention.

FIG. 1 shows a method for differentially setting data transaction rights by setting rights of nodes. The term “data transaction rights” may be used as a
20 meaning including an access/processing (reading, writing, etc.) right regarding specific data on a blockchain, a right to request a specific process in a blockchain network, and the like.

The present invention discloses a blockchain network structure for limitedly providing a data transaction right in a blockchain network to an external node by
25 setting the data transaction right of the external node in the blockchain network. In

this way, some rights for operation in the blockchain network may be given to the external node.

Referring to FIG. 1, a blockchain network may include nodes which may be server units constituting the blockchain network. The nodes in the blockchain network may be connected through a channel. Nodes may be connected through the same channel or different channels, and only nodes belonging to the same channel may be able to communicate with each other. Also, one node may have several channels.

For example, a first node 110, a second node 120, and a third node 130 may communicate through a first channel 160, and the third node 130, a fourth node 140, and a fifth node 150 may communicate through a second channel 170. The first node 110, the second node 120, and the third node 130 may be able to communicate with each other through the first channel 160, and the third node 130, the fourth node 140, and the fifth node 150 may be able to communicate with each other through the second channel 170. The third node 130 may have a data transaction right in the first channel 160 and the second channel 170. The first node 110 and the second node 120 may have a data transaction right in the first channel 160. The fourth node 140 and the fifth node 150 may have a data transaction right in the second channel 170. Separate blocks and blockchains may be generated for the channels. An additional channel may be managed as necessary so that an additional blockchain may be generated.

A chain code may be installed on a node, and a transaction that can be processed by the node may be determined on the basis of the chain code installed on the node. For example, between the first node 110 and the second node 120 connected through the first channel 160, chain code A and chain code B may be

installed on the first node 110, and chain code A may be installed on the second node 120.

In this case, the first node 110 may process transactions related to chain code A and chain code B, and the second node 120 may process transactions only related to chain code A. A chain code may be updated to different versions, and data subordinate to a specific chain code may be shared by nodes on which the chain code is installed.

Also, according to the exemplary embodiment of the present invention, data is classified, and data transaction rights may be limited according to nodes. Data may be classified as public data and private data. In a specific channel, a node on which a specific chain code is installed may have a data transaction right for public data. In the specific channel, among nodes on which the specific chain code is installed, only a node given an access right to private data may have a data transaction right to private data.

In other words, according to the exemplary embodiment of the present invention, a data transaction right of a node may be set on the basis of a channel, a channel code, and a data classification. Specifically, a data transaction right of a node may be limited by a channel, a channel code, and a data classification in sequence.

To have a data transaction right for data in a channel, a node should belong to the channel. Also, to have a data transaction right for data related to a chain code among pieces of data in the channel, the specific chain code should be installed on the node. Further, to have a data transaction right for data classified as private data among pieces of data related to the specific chain code in the specific channel, the node should be able to access private data.

Data transaction rights may be set in units of nodes of each channel, nodes of each chain code in a channel, and nodes specified in each chain code.

When a transaction of data shared in a specific channel occurs, an event of a change in data caused by the transaction may occur on all nodes which have a data transaction right for corresponding data in the channel.

When a transaction of data shared in a specific chain code in a specific channel occurs, an event of a change in data caused by the transaction may occur on nodes in the specific channel which have a data transaction right for the corresponding data and on which the specific chain code is installed.

When a transaction of private data shared in a specific code in a specific channel occurs, an event of a change in data may occur on nodes having a private data transaction right among nodes in the specific channel which have a data transaction right for the corresponding private data and on which the specific chain code is installed.

A method of processing a transaction by setting an external node of which such a hierarchical data access (or sharing) right is limited will be described below according to an exemplary embodiment of the present invention.

Although the exemplary embodiment of the present invention will be described on the basis of a transaction related to an asset trade for convenience of description, transactions related to information other than asset trades also fall within the scope of the present invention.

FIG. 2 is a conceptual diagram illustrating a method of processing a transaction which is caused by an external node according to an exemplary embodiment of the present invention.

FIG. 2 shows a method of processing a transaction caused by an external node on the basis of a transaction right setting.

Referring to FIG. 2, nodes in a blockchain network may be classified as internal nodes 200 and external nodes 210, 220. The external nodes 210 and 220 and the internal nodes 200 may have different data transaction rights. The internal nodes 200 may have a first data transaction right 250 in the blockchain network, and the external nodes 210 and 220 may have a second data transaction right 260 in the blockchain network.

The first data transaction right 250 may be a right broader than (or superior to) the second data transaction right 260, and some of data that can be accessed and/or processed with the first data transaction right 250 may not be accessed and/or processed with the second data transaction right 260.

The internal nodes 200, the first external node 210, and the second external node 220 may be assumed to be present in the blockchain network. The internal nodes 200 may have the first data transaction right 250, and the first external node 210 and the second external node 220 may have the second data transaction right 260. The first data transaction right 250 may be in a higher level than the second data transaction right 260.

For example, the second data transaction right 260 may include a data transaction right to generate trade request data and share the trade request data with other nodes which have the same or a higher-level data transaction right. The first data transaction right 250 may include not only a data transaction right to generate trade request data and share the trade request data with other nodes which have the same or a higher-level data transaction right but also a data transaction right to

process trade request data, determine validity of the trade request data, and change asset information.

The internal nodes 200, the first external node 210, or the second external node 220 may cause a transaction for generating and sharing trade request data according to the first data transaction right 250. For example, when the first external node 210 having the first data transaction right 250 generates trade request data, the second external node 220 and the internal nodes 200 having the same first data transaction right 250 may share the trade request data generated by the first external node 210.

The internal nodes 200 may process the trade request data and determine validity of the trade request data on the basis of the first data transaction right 250 and change asset information. The internal nodes 200 may determine validity of the trade request data using a transaction engine and change a personal asset when the trade request data is valid.

As a detailed example, the first external node 210 may generate trade request data for purchasing specific DABS traded at an exchange on the basis of the second data transaction right 260 and share the trade request data with the second external node 220 and the internal nodes 200. The first external node 210 may be a node of a service provider such as an external messenger service node or an external financial service node.

In other words, since the first data transaction right 250, which is a right to make a DABS trade request, is given to a node which provides a service, it is possible to make a DABS trade request not directly through an exchange but through a messenger service or a financial service, and a DABS transaction service may be provided in another existing service.

The trade request data generated by the first external node 210 may be shared with the second external node 220 and an internal node 200. The internal node 200 may be an exchange node, which may proceed with a DABS transaction on the basis of the shared trade request data and reflect results of the DABS transaction in asset details.

In other words, since the external nodes 210 and 220 are given a right to generate trade request data, a user can request a DABS transaction in an external service, and the requested DABS transaction may be processed. The user may be able to trade DABS even through a messenger service without directly accessing the exchange node.

Although a transaction related to DABS is illustrated in FIG. 2 for convenience of description, it may possible to use a blockchain-based service in the specific external nodes 210 and 220 by setting a limited data transaction right for the external nodes 210 and 220 not only with regard to a DABS transaction but also with regard to transactions having various other purposes.

Various methods may be used to set a limited data transaction right in the external nodes 210 and 220. As a method for setting a limited data transaction right in the external nodes 210 and 220, 1) a data classification method, 2) a chain code installation method, and 3) a channel classification method will be described in detail below according to exemplary embodiments of the present invention.

FIG. 3 is a conceptual diagram illustrating a method for setting a limited data transaction right in an external node according to an exemplary embodiment of the present invention.

FIG. 3 shows a method for setting a limited data transaction right on an external node on the basis of a data classification.

Referring to FIG. 3, when the same channel and the same chain code are installed on internal nodes 300 and external nodes 320, a data transaction right for corresponding data may be limited through data classifications such as first data (e.g., public data) and second data (e.g., private data). Data may be classified by giving a
5 separate identifier thereto or separately encrypting the data.

The internal nodes 300 have a data transaction right for first data and second data, and the external nodes 320 have a data transaction right for first data. In this case, the internal nodes 300 may generate a transaction for first data and second data to process the first data and the second data, and the external nodes 320 may generate
10 a transaction for first data to process the first data.

It may be assumed that first data is trade request data and second data is transaction management data. In this case, the external nodes 320 may generate a transaction for the trade request data and share the transaction with the internal nodes 300, and the internal nodes 300 may process the trade request data and generate and
15 process an asset management data transaction for managing an asset.

Even when the same channel and same chain code are used, differential data transaction rights are set on the basis of such data classifications so that the external nodes 320 may also be able to use some of blockchain-based services provided by the internal nodes 300.

20 FIG. 4 is a conceptual diagram illustrating a method for setting a limited data transaction right in an external node according to an exemplary embodiment of the present invention.

FIG. 4 shows a method for setting a limited data transaction right in an external node by installing a chain code.

Referring to FIG. 4, a first chain code may be installed on internal nodes 400, and a second chain code may be installed on external nodes 420.

A data transaction right for a trade request transaction and an asset management transaction may be given on the basis of the first chain code, and a data
5 transaction right for a trade request transaction may be given on the basis of the second chain code.

Therefore, the external nodes 420 on which the second chain code is installed may generate a trade request transaction, and the internal nodes 400 on which the first chain code is installed may verify validity of the trade request transaction and
10 generate an asset management transaction on the basis of the trade request transaction to change an asset.

On the basis of such node classifications through chain code installation, nodes connected through the same channel may operate with differentiated data transaction rights, and the external nodes 420 may also be able to use some of
15 blockchain-based services provided by the internal nodes 400.

FIG. 5 is a conceptual diagram illustrating a method for setting a limited data transaction right in an external node according to an exemplary embodiment of the present invention.

FIG. 5 shows a method for setting a limited data transaction right in an
20 external node on the basis of channel classifications.

Referring to FIG. 5, a first channel and a second channel are sorted out to set different data transaction rights in internal nodes 500 and external nodes 520.

The internal nodes 500 may be set to be able to communicate through the first channel and the second channel, and the external nodes 520 may be set to be able to
25 communicate only through the second channel.

The external node 520 may share trade request data using the second channel, and the internal nodes 500 may check the trade request data through the second channel. The internal nodes 500 may generate and process trade asset management data in the first channel on the basis of the trade request data checked through the
5 second channel.

In this way, it is possible to generate trade request data through the external nodes 520 and transfer the trade request data to the internal nodes 500 so that the trade request data may be processed.

FIG. 6 illustrates a method of hierarchically setting external nodes according
10 to an exemplary embodiment of the present invention.

FIG. 6 shows a method for setting a first level external node, a second level external node, and a third level external node on the basis of an internal node.

Referring to FIG. 6, the internal node, the first level external node, and the second level external node are connected through a first channel, and the third level
15 external node may be connected through a second channel. In this way, the third level external node may be separated from the internal node, the first level external node, and the second level external node, and the third level external node may perform limited operation in a blockchain network.

Among the internal node, the first level external node, and the second level
20 external node, channel code A may be set in the internal node and the first level external node, channel code B may be set in the second level external node. The internal node and the first level external node on which channel code A is set may share data related to channel code A, and the second level external node on which channel code B is set may share data related to channel code B. In this way, the
25 second level external node may be separated from the internal node and the first level

external node, and the second level external node may perform limited operation in the blockchain network.

Private data may be set so that only the internal node between the internal node and the first level external node may access the private data. In this case, only
5 the internal node can access the private data, and the first level external node may not access the private data. In this way, the internal node and the first level external node may be separated, and the first level external node may perform limited operation in the blockchain network.

Node-specific right setting according to the exemplary embodiments of the
10 present invention may be performed by a setup node. The setup node may include a communication unit which is implemented to communicate with an external node and a processor which is operatively connected to the communication unit. The processor may perform a node-specific right setting method.

A method of processing a transaction through an external node on a
15 blockchain according to an exemplary embodiment of the present invention may include a step in which a setup node sets internal nodes and external nodes, a step in which the setup node sets a first data transaction right on the internal nodes, and a step in which the setup node sets a second data transaction right on the external nodes. The first data transaction right may be a right that is set in the internal nodes
20 to operate in a blockchain network, and the second data transaction right may be a right that is set in the external nodes to operate in the blockchain network. As described above, the first data transaction right and the second data transaction right may be set on the basis of channels, channel codes, or data classifications.

When the first data transaction right and the second data transaction right are
25 set on the basis of channels, the internal nodes may be connected on the basis of the

first channel, and the external nodes may be connected on the basis of the second channel. The first channel and the second channel may be separated so that separate blockchains may be generated.

When the first data transaction right and the second data transaction right are set on the basis of chain codes, a first chain code may be installed on the internal nodes, and a second chain code may be installed on the external nodes. The internal nodes process data that is related to the first chain code, and the external nodes process data that is related to the second chain code. The first chain code may include a function of the second chain code.

FIG. 7 is a conceptual diagram illustrating a method of trading assets through an external node according to an exemplary embodiment of the present invention.

FIG. 7 shows a method of trading DABS through an external node which is assumed to be a messenger service operator.

Referring to FIG. 7, an external node is set for a messenger service operator, and a messenger service user may do a trade through a messenger 700. For example, a trade platform for trading DABS through the messenger 700 may be provided, and a DABS trade order may be made through the messenger 700 on the basis of the trade platform.

In other words, a data transaction right to generate a trade order may be set in the external node for the messenger service operator by a setup node so that a trade order may be generated without accessing an exchange node 720. As described above, the external node may set data transaction rights on the basis of channels, channel codes, and data classifications.

The trade order generated through the messenger 700 may be transferred to the exchange node 720 and processed by the exchange node 720 so that the trade

may be finished. When the trade is finished, the end of the trade may be reported through the messenger 700. In this way, it is possible to trade DABS, which are conventionally traded only by accessing an exchange, through an exchange node while using another service.

5 According to an exemplary embodiment of the present invention, a limited function may be given through a channel, and the channel may be limited through an independent channel connection and a virtual channel connection. When a plurality of nodes which will use the same channel are set with separate channels without interference of other nodes, a limited function may be set through the physically
10 separated channels. For example, when node A, node B, and node C may be connected as nodes in a channel without an intermediate node, node A, node B, and node C may be set as independent channels which are physically separated channels.

 However, when nodes in a channel are connected only through an intermediate node outside the channel because it is necessary to set the nodes with
15 the same channel, security of data delivered through the channel may be problematic. For example, when node A, node B, and node C are connected as nodes in a channel only through node X which is an intermediate node outside the channel, it is not possible to set physically separated channels. In this case, according to the exemplary embodiments of the present invention, it is possible to use a partial
20 channel section data separating encryption method for setting a node with an independent channel even when an intermediate node outside the channel is included.

 When it is necessary to transmit data through the intermediate node outside the channel, a section in which the data should be transmitted through the intermediate node outside the channel may be set as a data separating encryption
25 section, and data separating encryption may be performed in the data separating

encryption section. Specifically, data delivered from a node in the channel to the node outside the channel may be encrypted and delivered to a subsequent node in the channel in a bypass manner. In this case, encryption may be performed on the basis of an encryption key value included in previously transmitted data after initial
5 encryption. Therefore, only a node in the channel which decrypts the data that is previously transmitted while continuously varying can decrypt the encrypted data. There may be a plurality of data separating encryption sections, and different encryption key values may be separately applied to the plurality of data separating encryption sections. In this way, even when there is an intermediate node outside
10 the channel, nodes may be connected through a virtual independent channel.

The above-described embodiments of the present invention may be implemented as the form of a computer instruction that can be executed through various computer components and may be recorded in computer readable recording media. The computer readable recording media may include a program instruction,
15 a data file, and a data structure, and/or combinations thereof. The program instruction recorded in the computer readable recording media may be specially designed and prepared for the present invention or may be an available well-known instruction for those skilled in the field of computer software. Examples of the computer readable recording media include, for example, magnetic media such as a
20 hard disk, a floppy disk, and a magnetic tape, optical media such as a compact disc read only memory (CD-ROM) and a digital video disc (DVD), magneto-optical media such as a floptical disk, and a hardware device, such as a read only memory (ROM), a random access memory (RAM), or a flash memory, that is specially made to store and perform the program instruction. Examples of the program instruction
25 may include a machine code generated by a compiler and a high-level language code

that can be executed in a computer using an interpreter. Such a hardware device may be configured as at least one software module in order to perform operations of the present invention and vice versa.

While the present invention has been described with reference to specific
5 details such as detailed components, specific embodiments and drawings, these are only examples to facilitate overall understanding of the present invention and the present invention is not limited thereto. It will be understood by those skilled in the art that various modifications and alterations may be made.

Therefore, the spirit and scope of the present invention are defined not by the
10 detailed description of the present invention but by the appended claims and encompass all modifications and equivalents that fall within the scope of the appended claims.

[CLAIMS]

[Claim 1]

A method of processing a transaction through an external node on a blockchain, the method comprising:

- 5 setting, by a setup node, internal nodes and external nodes;
 setting, by the setup node, a first data transaction right in the internal nodes;
 and
 setting, by the setup node, a second data transaction right in the external
nodes,
10 wherein the first data transaction right is a right which is set in the internal
nodes to operate in a blockchain network, and
 the second data transaction right is a right which is set in the external nodes to
operate in the blockchain network.

[Claim 2]

- 15 The method of claim 1, wherein the first data transaction right and the second
data transaction right are set on the basis of channels, channel codes, or data
classifications.

[Claim 3]

- The method of claim 2, wherein when the first data transaction right and the
20 second data transaction right are set on the basis of the channels, the internal nodes
are connected through a first channel, and the external nodes are connected through a
second channel, and
 the first channel and the second channel are separated to generate separate
blockchains.

- 25 [Claim 4]

The method of claim 3, wherein when the first data transaction right and the second data transaction right are set on the basis of chain codes, a first chain code is installed on the internal nodes, and a second chain code is installed on the external nodes,

- 5 the internal nodes process data related to the first chain code,
 the external nodes process data related to the second chain code, and
 the first chain code includes a function of the second chain code.

[Claim 5]

A setup node for processing a transaction through an external node on a
10 blockchain, the setup node comprising:

 a communication unit implemented to communicate with an external node;
 and

 a processor operatively connected to the communication unit,
 wherein the processor is implemented to set internal nodes and external nodes,
15 set a first data transaction right in the internal nodes, and set a second data
transaction right in the external nodes,

 wherein the first data transaction right is a right which is set in the internal
nodes to operate in a blockchain network, and

 the second data transaction right is a right which is set in the external nodes to
20 operate in the blockchain network.

[Claim 6]

The setup node of claim 5, wherein the first data transaction right and the second data transaction right are set on the basis of channels, channel codes, or data classifications.

25 [Claim 7]

The setup node of claim 6, wherein when the first data transaction right and the second data transaction right are set on the basis of the channels, the internal nodes are connected through a first channel, and the external nodes are connected through a second channel, and

5 the first channel and the second channel are separated to generate separate blockchains.

[Claim 8]

The setup node of claim 7, wherein when the first data transaction right and the second data transaction right are set on the basis of chain codes, a first chain code
10 is installed on the internal nodes, and a second chain code is installed on the external nodes,

the internal nodes process data related to the first chain code,

the external nodes process data related to the second chain code, and

the first chain code includes a function of the second chain code.