

DATA PROCESSING METHOD AND APPARATUS FOR INNOMINATE DIGITAL SIGNATURE MESSAGE, DEVICE AND MEDIUM

TECHNICAL FIELD

5 **[0001]** The present application relates to the field of data processing and, in particular, to a data processing method and apparatus for an innominate digital signature message, a device and a medium.

BACKGROUND

10 **[0002]** With the development of science and technology, the emergence of a nominative digital signature messages has greatly improved efficiency in message data processing.

15 **[0003]** In the prior art, a digital signature message generally refers to a nominative digital signature message, which is a legal payment method and uses a digital signature and automatic verification technology for legality confirmation. In addition to a recipient user's name required, an account number, value data and date, encrypted information is implied on the nominative digital signature message. When using the nominative digital signature message, a sender user sends the digital signature message issued by the sender user himself to a recipient user directly via an e-mail. The recipient user takes out the digital signature message from an e-mail box, signs verification
20 information received with an electronic signature, and then sends the digital signature message via an e-mail to a server of a data processing agency for data processing.

20 **[0004]** However, in a scenario where information of the recipient user is uncertain, it is necessary to use an innominate digital signature message. The current data processing method for the nominative digital signature message is not applicable to the

innominate digital signature message, so there is an urgent need for a data processing method for the innominate digital signature message that can process data of the innominate digital signature message.

SUMMARY

5 **[0005]** Embodiments of the present application provide a data processing method and apparatus for an innominate digital signature message, a device and a medium, which are used to solve the problem that there is an urgent need for a data processing method for the innominate digital signature message that can process data of the innominate digital signature message because the current data processing method for a
10 nominative digital signature message is not applicable to an innominate digital signature message.

[0006] In a first aspect, an embodiment of the present application provides a data processing method for an innominate digital signature message, where the method is applied to an innominate digital signature message data management platform and
15 includes:

 receiving a data transfer-in request sent by a value data management platform, where the data transfer-in request includes a transfer-in data flow direction identifier and transfer-in value data, and the transfer-in data flow direction identifier is an innominate digital signature message data management platform identity or a
20 message identifier of an innominate digital signature message for which transfer-in is to be done;

 generating a first target innominate digital signature message and determining a message identifier and a message key of the first target innominate digital signature message, if the transfer-in data flow direction identifier is the innominate
25 digital signature message data management platform identity; and

 determining the transfer-in value data as value data of the first target innominate digital signature message.

[0007] In a specific implementation, the method also includes:

determining, according to the message identifier of the innominate digital signature message for which transfer-in is to be done, whether or not status of the innominate digital signature message for which transfer-in is to be done is available status, if the transfer-in data flow direction identifier is the message identifier of the
5 innominate digital signature message for which transfer-in is to be done; and

updating, according to the transfer-in value data, value data of the innominate digital signature message for which transfer-in is to be done, if the status of the innominate digital signature message for which transfer-in is to be done is the available status.

10 **[0008]** In a specific implementation, if the transfer-in data flow direction identifier is the innominate digital signature message data management platform identity, the data transfer-in request further includes signing-for duration information, and the signing-for duration information is a signing-for duration or an unlimited signing-for duration identifier, the method further includes:

15 using the signing-for duration information as signing-for duration information of the first target innominate digital signature message;

if the signing-for duration information is the signing-for duration, generating a backflow innominate digital signature message and determining a message identifier and a message key of the backflow innominate digital signature message,
20 where value data of the backflow innominate digital signature message is zero, and signing-for duration information of the backflow innominate digital signature message is the unlimited signing-for duration identifier;

establishing and then storing a corresponding relationship between the message identifier of the backflow innominate digital signature message and the
25 message identifier of the first target innominate digital signature message; and

according to a current time and the signing-for duration information of the first target innominate digital signature message, if monitoring that the first target innominate digital signature message has not been signed for within a time limit, updating status of the first target innominate digital signature message to be unavailable

status, and updating, according to the corresponding relationship between the message identifier of the backflow innominate digital signature message and the message identifier of the first target innominate digital signature message, the value data of the backflow innominate digital signature message to the value data of the first target
5 innominate digital signature message.

[0009] In a specific implementation, the method further includes:

in response to an operation from a user for retrieving an innominate digital signature message, obtaining a message identifier of a to-be-retrieved innominate digital signature message input by the user;

10 obtaining a retrieval result according to the message identifier, where the retrieval result includes one or more of status of the to-be-retrieved innominate digital signature message, value data of the to-be-retrieved innominate digital signature message, signing-for duration information of the to-be-retrieved innominate digital signature message, and a change record data set of the to-be-retrieved innominate
15 digital signature message; and

displaying the retrieval result.

[0010] In a specific implementation, the method further includes:

in response to an operation from a user for signing for an innominate digital signature message to a new message, obtaining an innominate digital signature message
20 data management platform identity of the user and, a message identifier of a to-be-signed-for innominate digital signature message and a message key of the to-be-signed-for innominate digital signature message and signing-for duration information input by the user;

verifying, according to the message identifier of the to-be-signed-for
25 innominate digital signature message and the message key of the to-be-signed-for innominate digital signature message, the to-be-signed-for innominate digital signature message to generate a first verification result;

if the first verification result is that verification is passed, generating, according to the signing-for duration information input by the user, a second target

innominate digital signature message, and determining a message identifier and a message key of the second target innominate digital signature message;

updating, according to the message identifier of the to-be-signed-for innominate digital signature message and the message key of the to-be-signed-for innominate digital signature message, status of the to-be-signed-for innominate digital signature message to be unavailable status; and

using value data of the to-be-signed-for innominate digital signature message as value data of the second target innominate digital signature message.

[0011] In a specific implementation, the verifying, according to the message identifier of the to-be-signed-for innominate digital signature message and the message key of the to-be-signed-for innominate digital signature message, the to-be-signed-for innominate digital signature message to generate the first verification result includes:

determining whether or not the message identifier of the to-be-signed-for innominate digital signature message matches the message key of the to-be-signed-for innominate digital signature message; and determining, according to the message identifier of the to-be-signed-for innominate digital signature message, whether or not the status of the to-be-signed-for innominate digital signature message is available status, and whether or not the value data of the to-be-signed-for innominate digital signature message is zero;

generating the first verification result that verification is passed, if the message identifier of the to-be-signed-for innominate digital signature message matches the message key of the to-be-signed-for innominate digital signature message and the status of the to-be-signed-for innominate digital signature message is the available status and the value data of the to-be-signed-for innominate digital signature message is not zero; and

generating the first verification result that verification is not passed, if the message identifier of the to-be-signed-for innominate digital signature message does not match the message key of the to-be-signed-for innominate digital signature message and/or the status of the to-be-signed-for innominate digital signature message is

unavailable status and/or the value data of the to-be-signed-for innominate digital signature message is zero.

[0012] In a specific implementation, the method further includes:

5 in response to an operation from a user for signing for an innominate digital signature message to an existing message, obtaining a message identifier of a to-be-signed-for innominate digital signature message and a message key of the to-be-signed-for innominate digital signature message and a message identifier of an innominate digital signature message for which transfer-in is to be done input by the user;

10 verifying, according to the message identifier of the to-be-signed-for innominate digital signature message, the message key of the to-be-signed-for innominate digital signature message and the message identifier of the innominate digital signature message for which transfer-in is to be done, both the to-be-signed-for innominate digital signature message and the innominate digital signature message for which transfer-in is to be done, to generate a second verification result;

15 if the second verification result is that verification is passed, updating, according to value data of the to-be-signed-for innominate digital signature message, value data of the innominate digital signature message for which transfer-in is to be done; and

20 updating, according to the message identifier of the to-be-signed-for innominate digital signature message and the message key of the to-be-signed-for innominate digital signature message, status of the to-be-signed-for innominate digital signature message to be unavailable status.

[0013] In a specific implementation, the verifying, according to the message identifier of the to-be-signed-for innominate digital signature message, the message key of the to-be-signed-for innominate digital signature message and the message identifier of the innominate digital signature message for which transfer-in is to be done, both the to-be-signed-for innominate digital signature message and the innominate digital signature message for which transfer-in is to be done, to generate the second verification result includes:

determining whether or not the message identifier of the to-be-signed-for innominate digital signature message matches the message key of the to-be-signed-for innominate digital signature message; and determining, according to the message identifier of the to-be-signed-for innominate digital signature message and the message
5 identifier of the innominate digital signature message for which transfer-in is to be done, whether or not the status of the to-be-signed-for innominate digital signature message is available status, whether or not the value data of the to-be-signed-for innominate digital signature message is zero, and whether or not status of the innominate digital signature message for which transfer-in is to be done is available status;

10 generating the second verification result that verification is passed, if the message identifier of the to-be-signed-for innominate digital signature message matches the message key of the to-be-signed-for innominate digital signature message and the status of the to-be-signed-for innominate digital signature message is the available status and the value data of the to-be-signed-for innominate digital signature
15 message is not zero and the status of the innominate digital signature message for which transfer-in is to be done is the available status; and

generating the second verification result that verification is not passed, if the message identifier of the to-be-signed-for innominate digital signature message does not match the message key of the to-be-signed-for innominate digital signature message
20 and/or the status of the to-be-signed-for innominate digital signature message is unavailable status and/or the value data of the to-be-signed-for innominate digital signature message is zero and/or the status of the innominate digital signature message for which transfer-in is to be done is unavailable status.

[0014] In a specific implementation, the method further includes:

25 in response to an operation from a user for splitting an innominate digital signature message, obtaining an innominate digital signature message data management platform identity of the user and, a message identifier of a to-be-split innominate digital signature message and a message key of the to-be-split innominate digital signature message, a total number of split innominate digital signature messages, and value data

of each of the split innominate digital signature messages and signing-for duration information of each of the split innominate digital signature messages input by the user;

verifying, according to the message identifier of the to-be-split innominate digital signature message and the message key of the to-be-split innominate digital signature message and the value data of each of the split innominate digital signature messages, the to-be-split innominate digital signature message to generate a third verification result;

if the third verification result is that verification is passed, generating, according to the total number of the split innominate digital signature messages and the value data and the signing-for duration information of each of the split innominate digital signature messages, the split innominate digital signature messages whose number is the total number, and determining a message identifier and a message key of each of the split innominate digital signature messages;

if a sum of value data of all the split innominate digital signature messages is equal to value data of the to-be-split innominate digital signature message, updating, according to the message identifier of the to-be-split innominate digital signature message and the message key of the to-be-split innominate digital signature message, status of the to-be-split innominate digital signature message to be unavailable status;

if the sum of the value data of all the split innominate digital signature messages is less than the value data of the to-be-split innominate digital signature message, determining a difference between the value data of the to-be-split innominate digital signature message and the sum of the value data of all the split innominate digital signature messages, as a first target difference; and

updating, according to the message identifier of the to-be-split innominate digital signature message and the message key of the to-be-split innominate digital signature message, the value data of the to-be-split innominate digital signature message to the first target difference.

[0015] In a specific implementation, the verifying, according to the message identifier of the to-be-split innominate digital signature message and the message key

of the to-be-split innominate digital signature message and the value data of each of the split innominate digital signature messages, the to-be-split innominate digital signature message to generate the third verification result includes:

determining whether or not the message identifier of the to-be-split
5 innominate digital signature message matches the message key of the to-be-split
innominate digital signature message; and determining, according to the message
identifier of the to-be-split innominate digital signature message and the value data of
each of the split innominate digital signature messages, whether or not the status of the
to-be-split innominate digital signature message is available status, whether or not the
10 value data of the to-be-split innominate digital signature message is zero, and whether
or not the sum of the value data of all the split innominate digital signature messages is
greater than the value data of the to-be-split innominate digital signature message;

generating the third verification result that verification is passed, if the
message identifier of the to-be-split innominate digital signature message matches the
15 message key of the to-be-split innominate digital signature message and the status of
the to-be-split innominate digital signature message is the available status and the value
data of the to-be-split innominate digital signature message is not zero and the sum of
the value data of all the split innominate digital signature messages is less than or equal
to the value data of the to-be-split innominate digital signature message; and

20 generating the third verification result that verification is not passed, if the
message identifier of the to-be-split innominate digital signature message does not
match the message key of the to-be-split innominate digital signature message and/or
the status of the to-be-split innominate digital signature message is the unavailable
status and/or the value data of the to-be-split innominate digital signature message is
25 zero and/or the sum of the value data of all the split innominate digital signature
messages is greater than the value data of the to-be-split innominate digital signature
message.

[0016] In a specific implementation, the method further includes:

for each of the split innominate digital signature messages,

if signing-for duration information of a split innominate digital signature message is a signing-for duration, generating a backflow innominate digital signature message and determining a message identifier and a message key of the backflow innominate digital signature message, where value data of the backflow innominate digital signature message is zero, and signing-for duration information of the backflow innominate digital signature message is an unlimited signing-for duration identifier;

establishing and then storing a corresponding relationship between the message identifier of the backflow innominate digital signature message and the message identifier of the split innominate digital signature message; and

according to a current time and the signing-for duration information of the split innominate digital signature message, if monitoring that the split innominate digital signature message has not been signed for within a time limit, updating status of the split innominate digital signature message to be unavailable status, and updating, according to the corresponding relationship between the message identifier of the backflow innominate digital signature message and the message identifier of the split innominate digital signature message, the value data of the backflow innominate digital signature message to value data of the split innominate digital signature message.

[0017] In a specific implementation, the method further includes:

in response to an operation from a user for merging innominate digital signature messages into a new message, obtaining an innominate digital signature message data management platform identity of the user and, message identifiers of a plurality of to-be-merged innominate digital signature messages and message keys of the plurality of to-be-merged innominate digital signature messages and signing-for duration information input by the user;

verifying, according to the message identifiers of the plurality of to-be-merged innominate digital signature messages and the message keys of the plurality of to-be-merged innominate digital signature messages, the plurality of to-be-merged innominate digital signature messages to generate a fourth verification result;

if the fourth verification result is that verification is passed, generating,

according to the signing-for duration information input by the user, a third target innominate digital signature message, and determining a message identifier and a message key of the third target innominate digital signature message;

5 updating, according to the message identifiers of the plurality of to-be-merged innominate digital signature messages and the message keys of the plurality of to-be-merged innominate digital signature messages, status of the plurality of to-be-merged innominate digital signature messages to be unavailable status; and

10 using a sum of value data of the plurality of to-be-merged innominate digital signature messages as value data of the third target innominate digital signature message.

[0018] In a specific implementation, the verifying, according to the message identifiers of the plurality of to-be-merged innominate digital signature messages and the message keys of the plurality of to-be-merged innominate digital signature messages, the plurality of to-be-merged innominate digital signature messages to
15 generate the fourth verification result includes:

determining whether or not a message identifier of each to-be-merged innominate digital signature message matches a message key of each to-be-merged innominate digital signature message; and determining, according to the message identifiers of the plurality of to-be-merged innominate digital signature messages,
20 whether or not the status of all the to-be-merged innominate digital signature messages is available status;

generating the fourth verification result that verification is passed, if the message identifier of each to-be-merged innominate digital signature message matches the message key of each to-be-merged innominate digital signature message and the
25 status of all the to-be-merged innominate digital signature messages is the available status; and

generating the fourth verification result that verification is not passed, if there is at least one to-be-merged innominate digital signature message whose message identifier and message key do not match each other and/or there is at least one to-be-

merged innominate digital signature message whose status is the unavailable status.

[0019] In a specific implementation, the method further includes:

if the signing-for duration information is a signing-for duration, generating a backflow innominate digital signature message and determining a message identifier and a message key of the backflow innominate digital signature message, where value data of the backflow innominate digital signature message is zero, and signing-for duration information of the backflow innominate digital signature message is an unlimited signing-for duration identifier;

establishing and then storing a corresponding relationship between the message identifier of the backflow innominate digital signature message and the message identifier of the third target innominate digital signature message; and

according to a current time and signing-for duration information of the third target innominate digital signature message, if monitoring that the third target innominate digital signature message has not been signed for within a time limit, updating status of the third target innominate digital signature message to be unavailable status, and updating, according to the corresponding relationship between the message identifier of the backflow innominate digital signature message and the message identifier of the third target innominate digital signature message, the value data of the backflow innominate digital signature message to the value data of the third target innominate digital signature message.

[0020] In a specific implementation, the method further includes:

in response to an operation from a user for merging an innominate digital signature message into an existing message, obtaining a message identifier of a fourth target innominate digital signature message and a message key of the fourth target innominate digital signature message and a message identifier of at least one to-be-merged innominate digital signature message and a message key of the at least one to-be-merged innominate digital signature message input by the user;

verifying, according to the message identifier of the fourth target innominate digital signature message and the message key of the fourth target innominate digital

signature message and the message identifier of the at least one to-be-merged innominate digital signature message and the message key of the at least one to-be-merged innominate digital signature message, both the fourth target innominate digital signature message and the at least one to-be-merged innominate digital signature message to generate a fifth verification result;

if the fifth verification result is that verification is passed, updating, according to value data of the at least one to-be-merged innominate digital signature message, value data of the fourth target innominate digital signature message; and

updating, according to the message identifier of the at least one to-be-merged innominate digital signature message and the message key of the at least one to-be-merged innominate digital signature message, status of the at least one to-be-merged innominate digital signature message to be unavailable status.

[0021] In a specific implementation, the verifying, according to the message identifier of the fourth target innominate digital signature message and the message key of the fourth target innominate digital signature message and the message identifier of the at least one to-be-merged innominate digital signature message and the message key of the at least one to-be-merged innominate digital signature message, both the fourth target innominate digital signature message and the at least one to-be-merged innominate digital signature message to generate the fifth verification result includes:

determining whether or not the message identifier of the fourth target innominate digital signature message matches the message key of the fourth target innominate digital signature message and whether or not the message identifier of each to-be-merged innominate digital signature message matches the message key of the each to-be-merged innominate digital signature message; and determining, according to the message identifier of the fourth target innominate digital signature message and the message identifier of the at least one to-be-merged innominate digital signature message, whether or not status of the fourth target innominate digital signature message is available status and whether or not status of all of the at least one to-be-merged innominate digital signature message is available status;

generating the fifth verification result that verification is passed, if the message identifier of the fourth target innominate digital signature message matches the message key of the fourth target innominate digital signature message and the message identifier of each to-be-merged innominate digital signature message matches
5 the message key of the each to-be-merged innominate digital signature message and the status of the fourth target innominate digital signature message is the available status and the status of all of the at least one to-be-merged innominate digital signature message is the available status; and

generating the fifth verification result that verification is not passed, if the
10 message identifier of the fourth target innominate digital signature message does not match the message key of the fourth target innominate digital signature message and/or there is at least one to-be-merged innominate digital signature message whose message identifier and message key do not match each other and/or the status of the fourth target innominate digital signature message is unavailable status and/or there is at least one
15 to-be-merged innominate digital signature message whose status is unavailable status.

[0022] In a specific implementation, the method further includes:

obtaining a data transfer-out request, where the data transfer-out request comprises transfer-out value data, a message identifier of an innominate digital signature message for which transfer-out is to be done and a message key of the to-be-
20 transferred-out innominate digital signature message, and a value data management platform identity, and the data transfer-out request is sent by the value data management platform, or, the data transfer-out request is generated, in response to a data transfer-out operation from a user, according to the transfer-out value data, the value data management platform identity, the message identifier of the innominate digital
25 signature message for which transfer-out is to be done and the message key of the innominate digital signature message for which transfer-out is to be done input by the user;

verifying, according to the message identifier of the innominate digital signature message for which transfer-out is to be done and the message key of the

innominate digital signature message for which transfer-out is to be done, the innominate digital signature message for which transfer-out is to be done to generate a sixth verification result;

5 if the sixth verification result is that verification is passed, sending a data transfer request to the value data management platform, wherein the data transfer request comprises the transfer-out value data and the value data management platform identity;

10 if value data of the innominate digital signature message for which transfer-out is to be done is greater than the transfer-out value data, determining a difference between the value data of the innominate digital signature message for which transfer-out is to be done and the transfer-out value data, as a second target difference;

15 updating, according to the message identifier of the innominate digital signature message for which transfer-out is to be done and the message key of the innominate digital signature message for which transfer-out is to be done, the value data of the innominate digital signature message for which transfer-out is to be done, to the second target difference; and

20 if the value data of the innominate digital signature message for which transfer-out is to be done is equal to the transfer-out value data, updating, according to the message identifier of the innominate digital signature message for which transfer-out is to be done and the message key of the innominate digital signature message for which transfer-out is to be done, status of the innominate digital signature message for which transfer-out is to be done to be unavailable status.

[0023] In a specific implementation, the verifying, according to the message identifier of the innominate digital signature message for which transfer-out is to be done and the message key of the innominate digital signature message for which transfer-out is to be done, the innominate digital signature message for which transfer-out is to be done to generate the sixth verification result includes:

determining whether or not the message identifier of the innominate digital signature message for which transfer-out is to be done matches the message key of the

innominate digital signature message for which transfer-out is to be done; and determining, according to the message identifier of the innominate digital signature message for which transfer-out is to be done, whether or not the status of the innominate digital signature message for which transfer-out is to be done is available status, and
5 whether or not the value data of the innominate digital signature message for which transfer-out is to be done is less than the transfer-out value data;

generating the sixth verification result that verification is passed, if the message identifier of the innominate digital signature message for which transfer-out is to be done matches the message key of the innominate digital signature message for
10 which transfer-out is to be done and the status of the innominate digital signature message for which transfer-out is to be done is the available status and the value data of the innominate digital signature message for which transfer-out is to be done is greater than or equal to the transfer-out value data; and

generating the sixth verification result that verification is not passed, if the message identifier of the innominate digital signature message for which transfer-out is
15 to be done does not match the message key of the innominate digital signature message for which transfer-out is to be done and/or the status of the innominate digital signature message for which transfer-out is to be done is the unavailable status and/or the value data of the innominate digital signature message for which transfer-out is to be done is
20 less than the transfer-out value data.

[0024] In a second aspect, an embodiment of the present application provides a data processing method for an innominate digital signature message, where the method is applied to a value data management platform and includes:

in response to a data transfer-in operation from a user, obtaining data
25 transfer-in information input by the user, where the data transfer-in information includes a value data management platform identity, a value data management platform password, a transfer-in data flow direction identifier and transfer-in value data, and the transfer-in data flow direction identifier is an innominate digital signature message data management platform identity or a message identifier of an innominate digital signature

message for which transfer-in is to be done;

transferring, according to the value data management platform identity and the value data management platform password and from an identity data set corresponding to the value data management platform identity, value data equal to the transfer-in value data into an innominate digital signature message general data set corresponding to an innominate digital signature message data management platform; and

10 sending a data transfer-in request to the innominate digital signature message data management platform, where the data transfer-in request includes the transfer-in data flow direction identifier and the transfer-in value data.

[0025] In a specific implementation, the method further includes:

in response to a data transfer-out operation from the user, obtaining transfer-out value data, the value data management platform identity, a message identifier of an innominate digital signature message for which transfer-out is to be done and a message key of the innominate digital signature message for which transfer-out is to be done input by the user; and

20 sending a data transfer-out request to the innominate digital signature message data management platform, where the data transfer-out request includes the transfer-out value data, the message identifier of the innominate digital signature message for which transfer-out is to be done and the message key of the innominate digital signature message for which transfer-out is to be done, and the value data management platform identity.

[0026] In a specific implementation, the method further includes:

25 receiving a data transfer request sent by the innominate digital signature message data management platform, where the data transfer request includes transfer-out value data and the value data management platform identity; and

transferring, according to the value data management platform identity and from the innominate digital signature message general data set corresponding to the innominate digital signature message data management platform, value data equal to

the transfer-out value data into the identity data set corresponding to the value data management platform identity.

[0027] In a third aspect, an embodiment of the present application provides a data processing apparatus for an innominate digital signature message, including:

5 a communicating module, configured to receive a data transfer-in request sent by a value data management platform, where the data transfer-in request includes a transfer-in data flow direction identifier and transfer-in value data, and the transfer-in data flow direction identifier is an innominate digital signature message data management platform identity or a message identifier of an innominate digital signature message for which transfer-in is to be done; and

a processing module, configured to:

generate a first target innominate digital signature message and determine a message identifier and a message key of the first target innominate digital signature message, if the transfer-in data flow direction identifier is the innominate digital signature message data management platform identity; and

15 determine the transfer-in value data as value data of the first target innominate digital signature message.

[0028] In a fourth aspect, an embodiment of the present application provides a data processing apparatus for an innominate digital signature message, including:

20 an obtaining module, configured to obtain, in response to a data transfer-in operation from a user, data transfer-in information input by the user, where the data transfer-in information includes a value data management platform identity, a value data management platform password, a transfer-in data flow direction identifier and transfer-in value data, and the transfer-in data flow direction identifier is an innominate digital signature message data management platform identity or a message identifier of an innominate digital signature message for which transfer-in is to be done;

a processing module, configured to transfer, according to the value data management platform identity and the value data management platform password and from an identity data set corresponding to the value data management platform identity,

value data equal to the transfer-in value data into an innominate digital signature message general data set corresponding to an innominate digital signature message data management platform; and

5 a communicating module, configured to send a data transfer-in request to the innominate digital signature message data management platform, where the data transfer-in request includes the transfer-in data flow direction identifier and the transfer-in value data.

[0029] In a fifth aspect, an embodiment of the present application provides an electronic device, including:

10 a processor, a memory, and a communication interface;
where the memory is used to store an instruction which is executable by the processor; and

the processor is configured to execute the data processing method for the innominate digital signature message according to any implementation of the first aspect by executing the instruction which is executable by the processor.

[0030] In a sixth aspect, an embodiment of the present application provides an electronic device, including:

a processor, a memory, and a communication interface;
where the memory is used to store an instruction which is executable by the
20 processor; and

the processor is configured to execute the data processing method for the innominate digital signature message according to any implementation of the second aspect by executing the instruction which is executable by the processor.

[0031] In a seventh aspect, an embodiment of the present application provides a
25 readable storage medium on which a computer program is stored, where when the computer program is executed by a processor, the data processing method for the innominate digital signature message according to any implementation of the first aspect or the second aspect is implemented.

[0032] In an eighth aspect, an embodiment of the present application provides a

computer program product, including a computer program, where when the computer program is executed by a processor, the data processing method for the innominate digital signature message according to any implementation of the first aspect or the second aspect when the computer program is implemented.

5 **[0033]** In the data processing method and apparatus for the innominate digital signature message, the device and the medium provided by embodiments of the present application, for performing data transfer-in processing for the innominate digital signature message, a value data management platform transfers, according to data transfer-in information input by a user, value data equal to transfer-in value data in the
10 data transfer-in information into an innominate digital signature message general data set corresponding to an innominate digital signature message data management platform, and then a data transfer-in request is sent to the innominate digital signature message data management platform. When determining that a transfer-in data flow direction identifier in the data transfer-in request is an innominate digital signature
15 message data management platform identity, the innominate digital signature message data management platform generates a first target innominate digital signature message, and determines a message identifier and a message key of the first target innominate digital signature message. In this solution, the data transfer-in processing for the innominate digital signature message is completed through the value data management
20 platform and the innominate digital signature message data management platform, realizing the data processing for the innominate digital signature message.

BRIEF DESCRIPTION OF DRAWINGS

[0034] In order to more clearly illustrate technical solutions in embodiments of the present application or in the prior art, in the following, the drawings required for the
25 description of the embodiments or the prior art will be briefly introduced. Obviously, the accompanying drawings in the following description show some embodiments of the present application. Persons of ordinary skill in the art may still derive other drawings based on these drawings without any creative effort.

- [0035]** FIG. 1 is a schematic flow diagram of Embodiment 1 of a data processing method for an innominate digital signature message provided by the present application.
- [0036]** FIG. 2 is a schematic flow diagram of Embodiment 2 of a data processing method for an innominate digital signature message provided by the present application.
- 5 **[0037]** FIG. 3 is a schematic flow diagram of Embodiment 3 of a data processing method for an innominate digital signature message provided by the present application.
- [0038]** FIG. 4 is a schematic flow diagram of Embodiment 4 of a data processing method for an innominate digital signature message provided by the present application.
- [0039]** FIG. 5 is a schematic flow diagram of Embodiment 5 of a data processing method for an innominate digital signature message provided by the present application.
- 10 **[0040]** FIG. 6 is a schematic flow diagram of Embodiment 6 of a data processing method for an innominate digital signature message provided by the present application.
- [0041]** FIG. 7 is a schematic flow diagram of Embodiment 7 of a data processing method for an innominate digital signature message provided by the present application.
- 15 **[0042]** FIG. 8 is a schematic flow diagram of Embodiment 8 of a data processing method for an innominate digital signature message provided by the present application.
- [0043]** FIG. 9 is a schematic flow diagram of Embodiment 9 of a data processing method for an innominate digital signature message provided by the present application.
- [0044]** FIG. 10 is a schematic flow diagram of Embodiment 10 of a data processing method for an innominate digital signature message provided by the present application.
- 20 **[0045]** FIG. 11 is a schematic flow diagram of Embodiment 11 of a data processing method for an innominate digital signature message provided by the present application.
- [0046]** FIG. 12 is a schematic flow diagram of Embodiment 12 of a data processing method for an innominate digital signature message provided by the present application.
- 25 **[0047]** FIG. 13 is a schematic flowchart of Embodiment 13 of a data processing method for innominate digital signature messages provided by the present application.
- [0048]** FIG. 14 is a schematic flowchart of Embodiment 14 of a data processing method for innominate digital signature messages provided by the present application.
- [0049]** FIG. 15 is a schematic flowchart of Embodiment 15 of a data processing

method for innominate digital signature messages provided by the present application.

[0050] FIG. 16 is a schematic structural diagram of Embodiment 1 of a data processing apparatus for an innominate digital signature message provided by the present application.

5 **[0051]** FIG. 17 is a schematic structural diagram of Embodiment 2 of a data processing apparatus for an innominate digital signature message provided by the present application.

[0052] FIG. 18 is schematic structural diagram I of an electronic device provided by the present application.

10 **[0053]** FIG. 19 is schematic structural diagram II of an electronic device provided in the present application.

DESCRIPTION OF EMBODIMENTS

[0054] In order to make the purposes, technical solutions and advantages of embodiments of the present application clearer, the technical solutions in the
15 embodiments of the present application will be clearly and comprehensively described below in conjunction with the drawings in the embodiments of the present application. Obviously, the described embodiments are some but not all of the embodiments of the present application. All other embodiments obtained by persons of ordinary skill in the art based on the embodiments in the present application and under teachings of these
20 embodiments shall fall within the protection scope of the present application.

[0055] In the specification, claims, and accompanying drawings of the present application, the terms “first”, “second”, “third”, “fourth”, and so on (if any) are intended to distinguish between similar objects but do not necessarily indicate a specific order or sequence. It is to be understood that data used in this way is interchangeable in a
25 suitable case, so that the embodiments of the present application described herein can be implemented in a sequence in addition to the sequence shown or described herein. Moreover, the terms “include”, “have”, and any other variants mean to cover the non-exclusive inclusion, for example, a process, method, system, product, or device that

includes a list of operations or units is not necessarily limited to those expressly listed operations or units, but may include other operations or units not expressly listed or inherent to such a process, method, system, product, or device.

[0056] With the development of science and technology, the nominative digital signature message is a legal payment method and uses digital signature and automatic verification technology for legality confirmation. In addition to a recipient user's name required, an account number, value data and date, encrypted information is implied on the nominative digital signature message. When using the nominative digital signature message, a sender user sends a digital signature message issued by the sender user himself to a recipient user directly via an e-mail. The recipient user takes out the digital signature message from an e-mail box, signs verification information received in the digital signature message with an electronic signature, and then sends the digital signature message via an e-mail to a server of a data processing agency for data processing.

[0057] However, in a scenario where information of the recipient user is uncertain, it is necessary to use an innominate digital signature message. The current data processing method for the nominative digital signature message is not applicable to the innominate digital signature message, so there is an urgent need for a data processing method for the innominate digital signature message that can process data of the innominate digital signature message.

[0058] Aiming at the problems existing in the prior art, in the process of researching the data processing method for the innominate digital signature message the inventor found that information of the recipient user is not required for the innominate digital signature message, so data processing for the innominate digital signature message can be performed with simply a message identifier and a message key, and further value data of all the innominate messages can be put into an innominate digital signature message general data set for unified processing. For data transfer-in processing, a value data management platform transfers value data equal to transfer-in value data input by a user into an innominate digital signature message general data set corresponding to

an innominate digital signature message data management platform, and then, a data transfer-in request is sent to the innominate digital signature message data management platform. The innominate digital signature message data management platform generates a new innominate digital signature message, and determines value data, a message identifier and a message key of this innominate digital signature message, thus completing the data transfer-in processing for the innominate digital signature message. Based on the above inventive concepts, a data processing solution for the innominate digital signature message in the present application is designed.

[0059] It should be noted that the value data management platform and the innominate digital signature message data management platform can be deployed on a terminal equipment, a server, a computer and other devices, which are not limited in embodiments of the present application and can be determined according to actual conditions.

[0060] An application scenario of the data processing method for the innominate digital signature message provided by the present application is illustrated below.

[0061] Illustratively, in the application scenario, a sender user needs to generate a digital signature message and send it to one of multiple recipient users, and then this recipient user, i.e., the target recipient user, signs for the digital signature message.

[0062] The sender user logs in to a value data management platform from a terminal equipment, and enters data transfer-in information. The data transfer-in information includes a value data management platform identity, a value data management platform password, a transfer-in data flow direction identifier and transfer-in value data. The transfer-in data flow direction identifier is an innominate digital signature message data management platform identity.

[0063] The value data management platform transfers, according to the value data management platform identity and the value data management platform password and from an identity data set corresponding to the value data management platform identity, value data equal to the transfer-in value data into an innominate digital signature message general data set corresponding to the innominate digital signature message

data management platform, and then sends a data transfer-in request to the innominate digital signature message data management platform. The data transfer-in request includes the transfer-in data flow direction identifier and the transfer-in value data.

5 **[0064]** Upon receiving the data transfer-in request, the innominate digital signature message data management platform generates a first target innominate digital signature message, and determines a message identifier of the first target innominate digital signature message, a message key of the first target innominate digital signature message and value data of the first target innominate digital signature message.

10 **[0065]** The first target innominate digital signature message is not dedicated to a designated recipient user. When the sender user determines a target recipient user, the first target innominate digital signature message may be sent to the target recipient user.

15 **[0066]** The sender user logs in to the innominate digital signature message data management platform from the terminal equipment, and then enters a recipient's innominate digital signature message data management platform identity and a to-be-sent innominate digital signature message. The to-be-sent innominate digital signature message at this time is the first target innominate digital signature message. After a click on "send", the innominate digital signature message data management platform sends the to-be-sent innominate digital signature message to a terminal equipment of the target recipient user.

20 **[0067]** The target recipient user logs in to the innominate digital signature message data management platform from a terminal equipment, and can view the innominate digital signature message, and then, sign for the innominate digital signature message. The innominate digital signature message data management platform can obtain an innominate digital signature message data management platform identity of the user, as well as a message identifier of a to-be-signed-for innominate digital signature message and a message key of the to-be-signed-for innominate digital signature message and signing-for duration information input by the user.

25 **[0068]** The innominate digital signature message data management platform verifies the to-be-signed-for innominate digital signature message, and generates a first

verification result; if the first verification result is that verification is passed, generates a second target innominate digital signature message according to the signing-for duration information input by the user and determines a message identifier and a message key of the second target innominate digital signature message; updates,
5 according to the message identifier of the to-be-signed-for innominate digital signature message and the message key of the to-be-signed-for innominate digital signature message, status of the to-be-signed-for innominate digital signature message to be unavailable status, uses value data of the to-be-signed-for innominate digital signature message as value data of the second target innominate digital signature message, thus
10 completing the signing-for of the to-be-signed-for innominate digital signature message.

[0069] It should be noted that the above scenario is only an example of an application scenario provided by an embodiment of the present application. Embodiments of the present application do not limit actual forms of various devices included in the scenario, nor the interaction mode between devices. These can be set
15 according to actual needs in a specific application of the solution.

[0070] Below, the technical solution of the present application will be described in detail through specific embodiments. It should be noted that the following specific embodiments may be combined with each other, and same or similar concepts or processes may not be repeated in some embodiments.

[0071] FIG. 1 is a schematic flow diagram of Embodiment 1 of a data processing method for an innominate digital signature message provided by the present application. This embodiment of the present application illustrates a case in which a value data management platform transfers, in response to a data transfer-in operation from a user, value data into an innominate digital signature message general data set corresponding
25 to an innominate digital signature message data management platform, and sends a data transfer-in request to the innominate digital signature message data management platform, and the innominate digital signature message data management platform generates an innominate digital signature message according to the data transfer-in request. The method in this embodiment may be implemented by software, hardware,

or a combination of software and hardware. As shown in FIG. 1, the data processing method for the innominate digital signature message specifically includes the following steps.

5 **[0072]** S101: the value data management platform obtains, in response to a data transfer-in operation from a user, data transfer-in information input by the user.

10 **[0073]** The user logs in to the value data management platform in order to perform data transfer-in operation and new message generation. At this time, the value data management platform that the user logged in to is a front end of the value data management platform. An interface for inputting data transfer-in information is displayed on an interface of the front end of the value data management platform. On this interface, the user enters the data transfer-in information including a value data management platform identity, a value data management platform password, a transfer-in data flow direction identifier, and transfer-in value data, etc.

15 **[0074]** In this step, the front end of the value data management platform obtains, in response to the user's data transfer-in operation, the data transfer-in information input by the user. The data transfer-in information includes the value data management platform identity, the value data management platform password, the transfer-in data flow direction identifier, and the transfer-in value data. The transfer-in data flow direction identifier is an innominate digital signature message data management platform identity or a message identifier of an innominate digital signature message for which transfer-in is to be done.

20 **[0075]** It should be noted that the user may directly input the data transfer-in information through manual input, or may select from options displayed on the interface for inputting data transfer-in information through a clicking operation to implement the input of the data transfer-in information. The way for the user to input the data transfer-in information is not limited in embodiments of the present application and can be determined according to an actual situation.

25 **[0076]** S102: the value data management platform transfers, according to the value data management platform identity and the value data management platform password

and from an identity data set corresponding to the value data management platform identity, value data equal to the transfer-in value data into an innominate digital signature message general data set corresponding to the innominate digital signature message data management platform.

5 **[0077]** In this step, after obtaining the data transfer-in information input by the user, the front end of the value data management platform sends a data transfer-in instruction to a back end of the value data management platform, where the data transfer-in instruction includes the data transfer-in information. According to the value data management platform identity and the value data management platform password, the
10 back end of the value data management platform transfers, from the identity data set corresponding to the value data management platform identity, the value data equal to the transfer-in value data into the innominate digital signature message general data set corresponding to the innominate digital signature message data management platform.

[0078] It should be noted that the back end of the value data management platform
15 may further verify whether or not the value data management platform identity in the data transfer-in information matches the value data management platform password in the data transfer-in information. If the value data management platform identity matches the value data management platform password, the back end of the value data management platform may further verify whether or not remaining value data in the
20 identity data set corresponding to the value data management platform identity is greater than or equal to the transfer-in value data in the data transfer-in information. If the remaining value data in the identity data set corresponding to the value data management platform identity is greater than or equal to the transfer-in value data in the data transfer-in information, the back end of the value data management platform
25 then transfers, from the identity data set corresponding to the value data management platform identity, the value data equal to the transfer-in value data into the innominate digital signature message general data set corresponding to the innominate digital signature message data management platform.

[0079] If the value data management platform identity does not match the value

data management platform password and/or the remaining value data in the identity data set corresponding to the value data management platform identity is less than the transfer-in value data in the data transfer-in information, the back end of the value data management platform may generate a verification failure message and send the
5 verification failure message to the front end of the value data management platform to display such message to the user.

[0080] S103: the value data management platform sends a data transfer-in request to the innominate digital signature message data management platform.

[0081] In this step, after the front end of the value data management platform
10 obtains the data transfer-in information input by the user, since an innominate digital signature message is generated on the innominate digital signature message data management platform, the back end of the value data management platform sends the data transfer-in request to a back end of the innominate digital signature message data management platform, where the data transfer-in request includes the transfer-in data
15 flow direction identifier and the transfer-in value data.

[0082] It should be noted that, with respect to an order of execution of steps S102 and S103, step S102 may be executed first, and then step S103 is executed; or, step S103 may be executed first, and then step S102 is executed; or, steps S102 and S103 are executed simultaneously. The order of execution of steps S102 and S103 is not
20 limited in embodiments of the present application and can be determined according to an actual situation.

[0083] S104: the innominate digital signature message data management platform receives the data transfer-in request sent by the value data management platform.

[0084] In this step, after the value data management platform sends the data
25 transfer-in request to the innominate digital signature message data management platform, the back end of the innominate digital signature message data management platform receives the data transfer-in request sent by the value data management platform. The data transfer-in request includes the transfer-in data flow direction identifier and the transfer-in value data. The transfer-in data flow direction identifier is

the innominate digital signature message data management platform identity or the message identifier of the innominate digital signature message for which transfer-in is to be done.

5 **[0085]** S105: the innominate digital signature message data management platform generates a first target innominate digital signature message and determines a message identifier and a message key of the first target innominate digital signature message, if the transfer-in data flow direction identifier is the innominate digital signature message data management platform identity.

10 **[0086]** In this step, after receiving the data transfer-in request, the back end of the innominate digital signature message data management platform judges whether the transfer-in data flow direction identifier is the innominate digital signature message data management platform identity or the message identifier of the innominate digital signature message for which transfer-in is to be done. If the transfer-in data flow direction identifier is the innominate digital signature message data management
15 platform identity, it means that a new innominate digital signature message needs to be generated. If the transfer-in data flow direction identifier is the message identifier of the innominate digital signature message for which transfer-in is to be done, it means that data needs to be transferred into an existing innominate digital signature message.

20 **[0087]** If the transfer-in data flow direction identifier is the innominate digital signature message data management platform identity, it means that a new innominate digital signature message needs to be generated. Accordingly, the back end of the innominate digital signature message data management platform generates the first target innominate digital signature message, and determines the message identifier and the message key of the first target innominate digital signature message.

25 **[0088]** It should be noted that the message identifier and the message key are unique, and the determined message identifier and message key may be determined according to one or more of a current time, the transfer-in value data, a random number, the innominate digital signature message data management platform identity, etc. The way of determining the message identifier and the message key is not limited in

embodiments of the present application and can be determined according to an actual situation.

5 **[0089]** S106: the innominate digital signature message data management platform determines the transfer-in value data as value data of the first target innominate digital signature message.

[0090] In this step, after generating the first target innominate digital signature message, the back end of the innominate digital signature message data management platform uses the transfer-in value data as the value data of the first target innominate digital signature message, thus completing the data transfer-in.

10 **[0091]** It should be noted that after generating the first target innominate digital signature message, the back end of the innominate digital signature message data management platform may further generate first data transfer-in record information according to the transfer-in value data and store the first data transfer-in record information in a change record data set of the first target innominate digital signature message. The first data transfer-in record information is used to indicate deposited value data, and the deposited value data is equal to the transfer-in value data. For all innominate digital signature messages in the innominate digital signature message data management platform, change record data sets of these innominate digital signature messages can be stored in a general data set, so that the back end of the innominate digital signature message data management platform can perform retrieving, modifying, deleting, adding and other processing for the data therein. A centralized database solution or a decentralized blockchain storage solution may be adopted for the general data set.

25 **[0092]** It should be noted that there may further be an incentive record data set in the innominate digital signature message data management platform. During the data transfer-in operation, according to a preset data transfer-in incentive mode, transfer-in incentive value data is determined and stored in the incentive record data set. Furthermore, if a source of preset incentive value data is the identity data set, the value data management platform transfers, from the identity data set corresponding to the

value data management platform identity, value data equal to the transfer-in incentive value data into the innominate digital signature message general data set corresponding to the innominate digital signature message management platform. If the source of the preset incentive value data is the innominate digital signature message, a difference
5 between the value data of the first target innominate digital signature message and the transfer-in incentive value data is used as updated value data of the first target innominate digital signature message, and record information is generated correspondingly and stored in the change record data set of the first target innominate digital signature message. The record information is used to indicate value data
10 transferred out to the incentive record data set. The value data transferred out is equal to the transfer-in incentive value data.

[0093] It should be noted that determining, according to the preset data transfer-in incentive mode, the transfer-in incentive value data may be as follows: using a product of the transfer-in value data and a preset ratio as the transfer-in incentive value data, or,
15 using preset transfer-in incentive value data as the transfer-in incentive value data, or, determining a transfer-in value data threshold range corresponding to the transfer-in value data, and then determining a preset ratio corresponding to the transfer-in value data threshold range, and finally using a product of the transfer-in value data and the preset ratio as the transfer-in incentive value data. The way of determining the transfer-
20 in incentive value data according to the preset data transfer-in incentive mode is not limited in embodiments of the present application and can be determined according to an actual situation.

[0094] In the data processing method for the innominate digital signature message provided by the embodiment, a value data management platform transfers, in response
25 to a data transfer-in operation from a user, value data into an innominate digital signature message general data set corresponding to an innominate digital signature message data management platform, and then sends a data transfer-in request to the innominate digital signature message data management platform, and the innominate digital signature message data management platform generates an innominate digital

signature message according to the data transfer-in request, and then determines a message identifier, a message key and value data corresponding to the innominate digital signature message. In comparison to the prior art in which information of a recipient user is required for a nominative digital signature message, the above solution
5 dispenses with the information of the recipient user, and realizes the data transfer-in processing for the innominate digital signature message.

[0095] FIG. 2 is a schematic flow diagram of Embodiment 2 of a data processing method for an innominate digital signature message provided by the present application. On the basis of the above-mentioned embodiments, this embodiment of the present
10 application illustrates a case in which the innominate digital signature message data management platform generates a backflow innominate digital signature message if the transfer-in data flow direction identifier is the innominate digital signature message data management platform identity and signing-for duration information is a signing-for duration. As shown in FIG. 2, the data processing method for the innominate digital
15 signature message specifically includes the following steps.

[0096] S201: use the signing-for duration information as signing-for duration information of the first target innominate digital signature message.

[0097] When a user enters the data transfer-in information on the value data management platform, if the transfer-in data flow direction identifier input by the user
20 is the innominate digital signature message data management platform identity, the data transfer-in information shall further include the signing-for duration information. A selection box for selecting whether there is a signing-for duration is further displayed on the interface for inputting data transfer-in information. If the user selects that there is the signing-for duration, a signing-for duration input box is displayed so that the user
25 enters a specific signing-for duration. The signing-for duration information obtained by the value data management platform is this signing-for duration. If the user selects that there is no signing-for duration, the signing-for duration information obtained by the value data management platform is an unlimited signing-for duration identifier. In addition, the data transfer-in request sent by the value data management platform to the

innominate digital signature message data management platform also includes the signing-for duration information.

[0098] In this step, after the back end of the innominate digital signature message data management platform generates the first target innominate digital signature message, if the transfer-in data flow direction identifier is the innominate digital signature message data management platform identity, the data transfer-in request further includes the signing-for duration information which is either the signing-for duration or the unlimited signing-for duration identifier. Furthermore, the back end of the innominate digital signature message data management platform uses the signing-for duration information as the signing-for duration information of the first target innominate digital signature message.

[0099] S202: if the signing-for duration information is the signing-for duration, generate a backflow innominate digital signature message and determine a message identifier and a message key of the backflow innominate digital signature message.

[0100] In this step, the back end of the innominate digital signature message data management platform judges whether the signing-for duration information is the signing-for duration or the unlimited signing-for duration identifier. If the signing-for duration information is the signing-for duration, it means that a backflow innominate digital signature message needs to be generated, so that the first target innominate digital signature message can be used for backflow when the first target innominate digital signature message has not been signed for within a time limit, so as to prevent data abnormality of the innominate digital signature message data management platform.

[0101] The back end of the innominate digital signature message data management platform generates the backflow innominate digital signature message. Value data of the backflow innominate digital signature message is zero, and signing-for duration information of the backflow innominate digital signature message is the unlimited signing-for duration identifier.

[0102] S203: establish and then store a corresponding relationship between the

message identifier of the backflow innominate digital signature message and the message identifier of the first target innominate digital signature message.

5 **[0103]** In this step, after the back end of the innominate digital signature message data management platform generates the backflow innominate digital signature message, the corresponding relationship between the message identifier of the backflow innominate digital signature message and the message identifier of the first target innominate digital signature message needs to be established and stored so that a corresponding backflow innominate digital signature message can be found for backflow.

10 **[0104]** S204: according to a current time and the signing-for duration information of the first target innominate digital signature message, if monitoring that the first target innominate digital signature message has not been signed for within a time limit, update status of the first target innominate digital signature message to be unavailable status, and update, according to the corresponding relationship between the message identifier
15 of the backflow innominate digital signature message and the message identifier of the first target innominate digital signature message, the value data of the backflow innominate digital signature message to the value data of the first target innominate digital signature message.

20 **[0105]** In this step, after the back end of the innominate digital signature message data management platform generates the backflow innominate digital signature message, according to the current time and the signing-for duration information of the first target innominate digital signature message, if the back end of the innominate digital signature message data management platform monitors that the first target innominate digital signature message has not been signed for within a time limit, that
25 is, the back end of the innominate digital signature message data management platform determines that the status of the first target innominate digital signature message is still available status when the current time reaches the signing-for duration after generation of the first target innominate digital signature message, indicating that the first target innominate digital signature message has not been signed-for within the time limit. In

this case, the back end of the innominate digital signature message data management platform updates status of the first target innominate digital signature message to be unavailable status, and finds, according to the corresponding relationship between the message identifier of the backflow innominate digital signature message and the message identifier of the first target innominate digital signature message, the backflow innominate digital signature message, and updates the value data of the backflow innominate digital signature message to the value data of the first target innominate digital signature message. Further, the back end of the innominate digital signature message data management platform may update the value data of the first target innominate digital signature message to zero.

[0106] It should be noted that the back end of the innominate digital signature message data management platform may further generate third data transfer-in record information according to the value data of the first target innominate digital signature message, and store the third data transfer-in record information in a change record data set of the value data of the backflow innominate digital signature message. The third data transfer-in record information is used to indicate value data transferred in from the first target innominate digital signature message, and the value data transferred in is equal to the value data of the first target innominate digital signature message. For the first target innominate digital signature message, corresponding record information may also be generated at this time, and stored in the change record data set of the value data of the first target innominate digital signature message to indicate value data transferred out to the backflow innominate digital signature message. The value data transferred out is equal to the value data of the first target innominate digital signature message.

[0107] It should be noted that if monitoring that the first target innominate digital signature message has been signed for within the time limit, that is, the back end of the innominate digital signature message data management platform determines that the status of the first target innominate digital signature message is updated to be unavailable status at a time within the signing-for duration after generation of the first target innominate digital signature message, indicating that the first target innominate

digital signature message has been signed-for within the time limit. In this case, the back end of the innominate digital signature message data management platform deletes the corresponding relationship between the message identifier of the backflow innominate digital signature message and the message identifier of the first target
5 innominate digital signature message.

[0108] In the data processing method for the innominate digital signature message provided by the embodiment, the backflow innominate digital signature message is generated if the transfer-in data flow direction identifier is the innominate digital signature message data management platform identity and the signing-for duration
10 information is the signing-for duration. Accordingly, in the case that through monitoring, the innominate digital signature message data management platform finds that the first target innominate digital signature message has not been signed for within the time limit, the innominate digital signature message data management platform updates the value data of the backflow innominate digital signature message. If monitoring that the first
15 target innominate digital signature message has been signed for within the time limit, the innominate digital signature message data management platform deletes the corresponding relationship between the message identifier of the backflow innominate digital signature message and the message identifier of the first target innominate digital signature message. In this way, incidence of data anomalies is effectively reduced.

[0109] FIG. 3 is a schematic flow diagram of Embodiment 3 of a data processing method for an innominate digital signature message provided by the present application. On the basis of the above-mentioned embodiments, this embodiment of the present application illustrates a case in which the innominate digital signature message data management platform performs transfer-in data processing when the transfer-in data
25 flow direction identifier is the message identifier of the innominate digital signature message for which transfer-in is to be done. As shown in FIG. 3, the data processing method for the innominate digital signature message specifically includes the following steps.

[0110] S301: if the transfer-in data flow direction identifier is the message identifier

of the innominate digital signature message for which transfer-in is to be done, the innominate digital signature message data management platform determines, according to the message identifier of the innominate digital signature message for which transfer-in is to be done, whether or not status of the innominate digital signature message for which transfer-in is to be done is available status; if the status of the innominate digital signature message for which transfer-in is to be done is the available status, step S302 is performed; if the status of the innominate digital signature message for which transfer-in is to be done is unavailable status, step S303 is performed.

[0111] In this step, after the back end of the innominate digital signature message data management platform receives the data transfer-in request sent by the value data management platform, if the transfer-in data flow direction identifier is the message identifier of the innominate digital signature message for which transfer-in is to be done, it means that data needs to be transferred into an existing innominate digital signature message. Thus, according to the message identifier of the innominate digital signature message for which transfer-in is to be done, the back end of the innominate digital signature message data management platform finds the innominate digital signature message for which transfer-in is to be done, and then determines whether or not the status of the innominate digital signature message for which transfer-in is to be done is available status.

[0112] It should be noted that the back end of the innominate digital signature message data management platform may first determine whether the corresponding innominate digital signature message into which the transfer-in value data is to be transferred can be found according to the message identifier of the innominate digital signature message for which transfer-in is to be done. If the innominate digital signature message for which transfer-in is to be done is found, the back end of the innominate digital signature message data management platform then judges whether or not the status of the innominate digital signature message for which transfer-in is to be done is available status. If the innominate digital signature message for which transfer-in is to be done is not found, a prompt message of data transfer-in failure may be sent to the

value data management platform so that the user can have a check.

[0113] S302: the innominate digital signature message data management platform updates, according to the transfer-in value data, value data of the innominate digital signature message for which transfer-in is to be done.

5 **[0114]** In this step, if the back end of the innominate digital signature message data management platform determines that the status of the innominate digital signature message for which transfer-in is to be done is available status, it means that the innominate digital signature message for which transfer-in is to be done can still be used and is not abandoned. In this case, the back end of the innominate digital signature
10 message data management platform updates, according to the transfer-in value data, the value data of the innominate digital signature message for which transfer-in is to be done, that is, adds the value data of the innominate digital signature message for which transfer-in is to be done and the transfer-in value data together to obtain updated value data of the innominate digital signature message for which transfer-in is to be done.

15 **[0115]** It should be noted that the back end of the innominate digital signature message data management platform may further generate second data transfer-in record information according to the transfer-in value data, and store the second data transfer-in record information in a change record data of the innominate digital signature message for which transfer-in is to be done. The second data transfer-in record
20 information is used to indicate deposited value data, and the deposited value data is equal to the transfer-in value data.

[0116] S303: the innominate digital signature message data management platform generates a prompt message of data transfer-in failure.

[0117] S304: the innominate digital signature message data management platform
25 sends the prompt message of data transfer-in failure to the value data management platform.

[0118] In the above steps, if the back end of the innominate digital signature message data management platform determines that the status of the innominate digital signature message for which transfer-in is to be done is unavailable status, it means that

the innominate digital signature message for which transfer-in is to be done has been abandoned and thus the data transfer-in processing cannot be performed, so it is necessary to generate the prompt message of data transfer-in failure to inform the user of the data transfer-in failure. Therefore, the prompt message of data transfer-in failure
5 is sent to the back end of the value data management platform.

[0119] S305: the value data management platform receives and displays the prompt message of data transfer-in failure sent by the innominate digital signature message data management platform.

[0120] In this step, after the innominate digital signature message data management
10 platform sends the prompt message of data transfer-in failure to the value data management platform, the back end of the value data management platform can receive the prompt message of data transfer-in failure, and then send the prompt message of data transfer-in failure to the front end of the value data management platform. The front end of the value data management platform receives and then displays the prompt
15 message of data transfer-in failure so that the user can have a check.

[0121] It should be noted that there may further be an incentive record data set in the innominate digital signature message data management platform. During the data transfer-in operation, according to a preset data transfer-in incentive mode, transfer-in incentive value data is determined and stored in the incentive record data set.
20 Furthermore, if a source of preset incentive value data is the identity data set, the value data management platform transfers, from the identity data set corresponding to the value data management platform identity, value data equal to the transfer-in incentive value data into the innominate digital signature message general data set corresponding to the innominate digital signature message management platform. If the source of the
25 preset incentive value data is the innominate digital signature message, a difference between the value data of the innominate digital signature message for which transfer-in is to be done and the transfer-in incentive value data is used as updated value data of the innominate digital signature message for which transfer-in is to be done, and record information is generated correspondingly and stored in a change record data set of the

innominate digital signature message for which transfer-in is to be done. The record information is used to indicate value data transferred out to the incentive record data set. The value data transferred out is equal to the transfer-in incentive value data.

[0122] It should be noted that determining, according to the preset data transfer-in incentive mode, the transfer-in incentive value data may be as follows: using a product of the transfer-in value data and a preset ratio as the transfer-in incentive value data, or, using preset transfer-in incentive value data as the transfer-in incentive value data, or, determining a transfer-in value data threshold range corresponding to the transfer-in value data, and then determining a preset ratio corresponding to the transfer-in value data threshold range, and finally using a product of the transfer-in value data and the preset ratio as the transfer-in incentive value data. The way of determining the transfer-in incentive value data according to the preset data transfer-in incentive mode is not limited in embodiments of the present application and can be determined according to an actual situation.

[0123] In the data processing method for the innominate digital signature message provided by the embodiment, when the transfer-in data flow direction identifier is the message identifier of the innominate digital signature message for which transfer-in is to be done, the value data of the innominate digital signature message for which transfer-in is to be done is updated if the status of the innominate digital signature message for which transfer-in is to be done is available status; and the prompt message of data transfer-in failure is generated if the status of the innominate digital signature message for which transfer-in is to be done is unavailable status. In this way, data transfer-in processing for an innominate digital signature message is implemented, and the normal operation of the innominate digital signature message data management platform and the value data management platform is also ensured.

[0124] FIG. 4 is a schematic flow diagram of Embodiment 4 of a data processing method for an innominate digital signature message provided by the present application. On the basis of the above-mentioned embodiments, this embodiment of the present application illustrates a case in which the innominate digital signature message data

management platform implements sending of the innominate digital signature message. As shown in FIG. 4, the data processing method for the innominate digital signature message specifically includes the following steps.

5 [0125] S401: in response to an operation from a sender user for sending an innominate digital signature message, obtain a recipient's innominate digital signature message data management platform identity and a to-be-sent innominate digital signature message input by the sender user.

10 [0126] The sender user logs in to the front end of the innominate digital signature message data management platform, inputs the recipient's innominate digital signature message data management platform identity and the to-be-sent innominate digital signature message in an interface for sending an innominate digital signature message, and clicks a "Send" button.

15 [0127] In this step, after the sender user clicks the "Send" button, the front end of the innominate digital signature message data management platform can obtain the recipient's innominate digital signature message data management platform identity and the to-be-sent innominate digital signature message input by the sender user. Then, the front end of the innominate digital signature message data management platform sends the recipient's innominate digital signature message data management platform identity and the to-be-sent innominate digital signature message input by the sender user to the back end of the innominate digital signature message data management platform.

20 [0128] It should be noted that the sender user may directly input the recipient's innominate digital signature message data management platform identity and the to-be-sent innominate digital signature message through manual input, or may select from options displayed on the interface for sending the innominate digital signature message through a clicking operation to implement the input of the recipient's innominate digital signature message data management platform identity and the to-be-sent innominate digital signature message. The way for the sender user to input the recipient's innominate digital signature message data management platform identity and the to-be-

sent innominate digital signature message is not limited in embodiments of the present application and can be determined according to an actual situation.

[0129] S402: in response to an operation from the recipient user for checking an innominate digital signature message, display message information of the to-be-sent
5 innominate digital signature message.

[0130] In this step, after the back end of the innominate digital signature message data management platform receives the recipient's innominate digital signature message data management platform identity and the to-be-sent innominate digital signature message, the recipient user can check the to-be-sent innominate digital
10 signature message. The recipient user logs in to the front end of the innominate digital signature message data management platform to perform the operation for checking the innominate digital signature message. The front end of the innominate digital signature message data management platform sends a checking request to the back end of the innominate digital signature message data management platform. The back end of the
15 innominate digital signature message data management platform sends message information such as a message identifier and a message key of the to-be-sent innominate digital signature message to the front end of the innominate digital signature message data management platform for display.

[0131] It should be noted that when the sender user directly inputs the to-be-sent
20 innominate digital signature message through manual input, the message identifier and the message key of the to-be-sent innominate digital signature message need to be input. The back end of the innominate digital signature message data management platform may further verify whether or not the message identifier matches the message key. If the message identifier does not match the message key, the back end of the innominate
25 digital signature message data management platform generates a sending failure prompt message, and sends the sending failure prompt message to the front end of the innominate digital signature message data management platform. Then, the front end of the innominate digital signature message data management platform displays the sending failure prompt message for the sender user to have a check.

[0132] The recipient user can log in to the front end of the innominate digital signature message data management platform to perform the operation for checking the innominate digital signature message. The front end of the innominate digital signature message data management platform sends the recipient user's innominate digital signature message data management platform identity to the back end of the innominate digital signature message data management platform. Accordingly, the back end of the innominate digital signature message data management platform can retrieve a corresponding innominate digital signature message, and then send information such as a message identifier and a message key and value data of the innominate digital signature message to the front end of the innominate digital signature message data management platform for display, so that the user can have a check.

[0133] It should be noted that there may further be an incentive record data set in the innominate digital signature message data management platform. During the operation of sending the innominate digital signature message, according to a preset sending incentive mode, sending incentive value data is determined and stored in the incentive record data set. A difference between the value data of the to-be-sent innominate digital signature message and the sending incentive value data is used as updated value data of the to-be-sent innominate digital signature message, and record information is generated correspondingly and stored in a change record data set of the to-be-sent innominate digital signature. The record information is used to indicate value data transferred out to the incentive record data set, and the value data transferred out is equal to the sending incentive value data.

[0134] It should be noted that determining, according to the preset sending incentive mode, the sending incentive value data may be as follows: using a product of the value data of the to-be-sent innominate digital signature message and a preset ratio as the sending incentive value data, or, using preset sending incentive value data as the sending incentive value data, or, determining a sending value data threshold range corresponding to the value data of the to-be-sent innominate digital signature message, and then determining a preset ratio corresponding to the sending value data threshold

range, and finally using a product of the value data of the to-be-sent innominate digital signature message and the preset ratio as the sending incentive value data. The way of determining the sending incentive value data according to the preset sending incentive mode is not limited in embodiments of the present application and can be determined
5 according to an actual situation.

[0135] It should be noted that the innominate digital signature message may also be sent or delivered by an email, a short message, or an instant messaging software, along with the message identifier and the message key, or, the message identifier and the message key may be recorded on an object such as a paper and a card through printing
10 or writing, and then this object is delivered to the recipient user. The way of delivering the innominate digital signature message is not limited in embodiments of the present application and can be determined according to an actual situation.

[0136] In the data processing method for the innominate digital signature message provided in the embodiment, to send the innominate digital signature message, the user
15 inputs the recipient's innominate digital signature message data management platform identity and the to-be-sent innominate digital signature message at the front end of the innominate digital signature message data management platform. Then the innominate digital signature message data management platform can obtain such data. Thus when the recipient user checks the innominate digital signature message, the innominate
20 digital signature message data management platform displays the message information of the innominate digital signature message. In this way, sending of the innominate digital signature message is implemented.

[0137] FIG. 5 is a schematic flow diagram of Embodiment 5 of a data processing method for an innominate digital signature message provided by the present application.
25 On the basis of the above-mentioned embodiments, this embodiment of the present application illustrates a case in which the innominate digital signature message data management platform implements retrieval of the innominate digital signature message. As shown in FIG. 5, the data processing method for the innominate digital signature message specifically includes the following steps.

[0138] S501: in response to an operation from a user for retrieving an innominate digital signature message, obtain a message identifier of a to-be-retrieved innominate digital signature message input by the user.

[0139] To retrieve information about an innominate digital signature message, a user can log in to the front end of the innominate digital signature message data management platform, enter the message identifier of the to-be-retrieved innominate digital signature message, and click a "Retrieve" button.

[0140] The front end of the innominate digital signature message data management platform obtains, in response to the operation from the user for retrieving the innominate digital signature message, a message identifier of a to-be-retrieved innominate digital signature message input by the user, and then sends this message identifier to the back end of the innominate digital signature message data management platform.

[0141] It should be noted that the user may directly input the message identifier of the to-be-retrieved innominate digital signature message through manual input, or may select from options displayed on an input interface through a clicking operation to implement the input of the message identifier. The way for the user to input the message identifier of the to-be-retrieved innominate digital signature message is not limited in embodiments of the present application and can be determined according to an actual situation.

[0142] S502: obtain a retrieval result according to the message identifier.

[0143] In this step, after receiving the message identifier of the to-be-retrieved innominate digital signature message, the back end of the innominate digital signature message data management platform retrieves the corresponding innominate digital signature message according to the message identifier, and then obtains the retrieval result. The retrieval result includes one or more of status of the to-be-retrieved innominate digital signature message, value data of the to-be-retrieved innominate digital signature message, signing-for duration information of the to-be-retrieved innominate digital signature message, and a change record data set of the to-be-

retrieved innominate digital signature message. Then the back end of the innominate digital signature message data management platform sends the retrieval result to the front end of the innominate digital signature message data management platform.

[0144] It should be noted that if the back end of the innominate digital signature message data management platform fails to find the corresponding innominate digital signature message according to the message identifier, the back end of the innominate digital signature message data management platform generates a retrieval failure prompt message and sends the retrieval failure prompt message to the front end of the innominate digital signature message data management platform for display, so that the user can have a check.

[0145] S503: display the retrieval result.

[0146] In this step, after receiving the retrieval result, the front end of the innominate digital signature message data management platform may display the retrieval result so that the user can have a check.

[0147] In the data processing method for the innominate digital signature message provided in the embodiment, retrieval of related data information of the innominate digital signature message can be implemented through the innominate digital signature message data management platform, improving the user experience. Furthermore, this process does not involve a change of value data in the innominate digital signature message general data set, thus effectively improving the security.

[0148] FIG. 6 is a schematic flow diagram of Embodiment 6 of a data processing method for an innominate digital signature message provided by the present application. On the basis of the above-mentioned embodiments, this embodiment of the present application illustrates a case in which the innominate digital signature message data management platform performs signing-for of the innominate digital signature message to a new innominate digital signature message. As shown in FIG. 6, the data processing method for the innominate digital signature message specifically includes the following steps.

[0149] S601: in response to an operation from a user for signing for an innominate

digital signature message to a new message, obtain an innominate digital signature message data management platform identity of the user and, a message identifier of a to-be-signed-for innominate digital signature message and a message key of the to-be-signed-for innominate digital signature message and signing-for duration information
5 input by the user.

[0150] When getting an innominate digital signature message, a user can sign for it on the innominate digital signature message data management platform. The user logs in to the front end of the innominate digital signature message data management platform and enters, on a signing-for interface, the message identifier and the message
10 key of the to-be-signed-for innominate digital signature message, and the signing-for duration information.

[0151] In this step, the front end of the innominate digital signature message data management platform obtains, in response to the operation from the user for signing for the innominate digital signature message to the new message, the message identifier and the message key of the to-be-signed-for innominate digital signature message and
15 the signing-for duration information input by the user, and the innominate digital signature message data management platform identity of the user, and sends such information to the back end of the innominate digital signature message data management platform.

[0152] It should be noted that the user may directly input the message identifier and the message key of the to-be-signed-for innominate digital signature message and the signing-for duration information through manual input, or may select from options displayed on the signing-for interface through a clicking operation to implement the input of the message identifier and the message key of the to-be-signed-for innominate
20 digital signature message and the signing-for duration information. The way for the user to input the message identifier and the message key of the to-be-signed-for innominate digital signature message and the signing-for duration information is not limited in embodiments of the present application and can be determined according to an actual situation.

[0153] S602: verify, according to the message identifier of the to-be-signed-for innominate digital signature message and the message key of the to-be-signed-for innominate digital signature message, the to-be-signed-for innominate digital signature message to generate a first verification result.

- 5 **[0154]** In this step, after receiving the message identifier and the message key of the to-be-signed-for innominate digital signature message, the signing-for duration information and the innominate digital signature message data management platform identity of the user, the back end of the innominate digital signature message data management platform first finds, according to the message identifier of the to-be-
10 signed-for innominate digital signature message, the corresponding to-be-signed-for innominate digital signature message, and then verifies the to-be-signed-for innominate digital signature message to generate the first verification result.

- [0155]** Specifically, according to the message identifier of the to-be-signed-for innominate digital signature message, the back end of the innominate digital signature
15 message data management platform finds the corresponding to-be-signed-for innominate digital signature message, and determines: whether or not the message identifier of the to-be-signed-for innominate digital signature message matches the message key of the to-be-signed-for innominate digital signature message, and then whether or not the status of the to-be-signed-for innominate digital signature message
20 is available status, and whether or not value data of the to-be-signed-for innominate digital signature message is zero.

- [0156]** If the message identifier of the to-be-signed-for innominate digital signature message matches the message key of the to-be-signed-for innominate digital signature message and the status of the to-be-signed-for innominate digital signature message is
25 the available status and the value data of the to-be-signed-for innominate digital signature message is not zero, the back end of the innominate digital signature message data management platform generates the first verification result that verification is passed.

[0157] If the message identifier of the to-be-signed-for innominate digital signature

message does not match the message key of the to-be-signed-for innominate digital signature message and/or the status of the to-be-signed-for innominate digital signature message is unavailable status and/or the value data of the to-be-signed-for innominate digital signature message is zero, the back end of the innominate digital signature message data management platform generates the first verification result that verification is not passed.

[0158] S603: determine whether the first verification result is that verification is passed; if the first verification result is that verification is passed, execute step S604; if the first verification result is that verification is not passed, execute step S607.

10 **[0159]** In this step, after generating the first verification result, in order to determine whether a process of signing for the innominate digital signature message can be continued, the back end of the innominate digital signature message data management platform needs to judge whether the first verification result is that verification is passed.

[0160] S604: generate a second target innominate digital signature message according to the signing-for duration information input by the user, and determine a message identifier and a message key of the second target innominate digital signature message.

[0161] S605: update, according to the message identifier of the to-be-signed-for innominate digital signature message and the message key of the to-be-signed-for innominate digital signature message, status of the to-be-signed-for innominate digital signature message to be unavailable status.

[0162] S606: use value data of the to-be-signed-for innominate digital signature message as value data of the second target innominate digital signature message.

25 **[0163]** In the above steps, if the back end of the innominate digital signature message data management platform judges that the first verification result is that verification is passed, it means that the process of signing for the innominate digital signature message can be continued. The back end of the innominate digital signature message data management platform then generates the second target innominate digital signature message according to the signing-for duration information input by the user,

that is, uses the signing-for duration information input by the user as signing-for duration information of the second target innominate digital signature message, and determines the message identifier and the message key of the second target innominate digital signature message.

5 **[0164]** Accordingly, the back end of the innominate digital signature message data management platform can find the to-be-signed-for innominate digital signature message according to the message identifier of the to-be-signed-for innominate digital signature message and the message key of the to-be-signed-for innominate digital signature message, and gets permission to perform data processing for the to-be-signed-
10 for innominate digital signature message, and updates the status of the to-be-signed-for innominate digital signature message to be unavailable status.

[0165] For the second target innominate digital signature message, the value data of the to-be-signed-for innominate digital signature message is used as the value data of the second target innominate digital signature message.

15 **[0166]** In addition, the value data of the to-be-signed-for innominate digital signature message may also be updated to zero.

[0167] It should be noted that the back end of the innominate digital signature message data management platform may further generate a signing-for result that signing-for is successful, and then send the signing-for result to the front end of the
20 innominate digital signature message data management platform for display, so that the user can have a check.

[0168] It should be noted that the back end of the innominate digital signature message data management platform may further generate first signing-for record information according to the value data of the to-be-signed-for innominate digital
25 signature message, and store the first signing-for record information in a change record data set of the to-be-signed-for innominate digital signature message. The first signing-for record information is used to indicate value data transferred out to the second target innominate digital signature message. The value data transferred out is equal to the value data of the to-be-signed-for innominate digital signature message.

[0169] According to the value data of the to-be-signed-for innominate digital signature message, second signing-for record information is generated and stored in a change record data set of the second target innominate digital signature message. The second signing-for record information is used to indicate value data transferred in from the to-be-signed-for innominate digital signature message. The value data transferred in is equal to the value data of the to-be-signed-for innominate digital signature message.

[0170] S607: generate a signing-for result.

[0171] S608: display the signing-for result.

[0172] In the above steps, if the back end of the innominate digital signature message data management platform judges that the first verification result is that verification is not passed, it means that the process of signing for the innominate digital signature message cannot be continued. The signing-for result that signing-for fails is generated and then sent to the front end of the innominate digital signature message data management platform for display, so that the user can have a check.

[0173] It should be noted that there may further be an incentive record data set in the innominate digital signature message data management platform. During the signing-for operation, according to a preset signing-for incentive mode, signing-for incentive value data is determined and stored in the incentive record data set. A difference between the value data of the second target innominate digital signature message and the signing-for incentive value data is used as updated value data of the second target innominate digital signature message, and record information is generated correspondingly and stored in the change record data set of the second target innominate digital signature message. The record information is used to indicate value data transferred out to the incentive record data set, and the value data transferred out is equal to the signing-for incentive value data.

[0174] It should be noted that determining, according to the preset signing-for incentive mode, the signing-for incentive value data may be as follows: using a product of the value data of the to-be-signed-for innominate digital signature message and a preset ratio as the signing-for incentive value data, or, using preset signing-for incentive

value data as the signing-for incentive value data, or, determining a signing-for value data threshold range corresponding to the value data of the to-be-signed-for innominate digital signature message, and then determining a preset ratio corresponding to the signing-for value data threshold range, and finally using a product of the value data of the to-be-signed-for innominate digital signature message and the preset ratio as the signing-for incentive value data. The way of determining the signing-for incentive value data according to the preset data signing-for incentive mode is not limited in embodiments of the present application and can be determined according to an actual situation.

[0175] In the data processing method for the innominate digital signature message provided by the embodiment, signing-for of the innominate digital signature message, especially signing-for of the innominate digital signature message to a new innominate digital signature message, can be implemented through the innominate digital signature message data management platform, without the information of the recipient user. Furthermore, this process does not involve a change of value data in the innominate digital signature message general data set, thus effectively improving the security.

[0176] FIG. 7 is a schematic flow diagram of Embodiment 7 of a data processing method for an innominate digital signature message provided by the present application. On the basis of the above-mentioned embodiments, this embodiment of the present application illustrates a case in which the innominate digital signature message data management platform generates a backflow innominate digital signature message if the signing-for duration information of the second target innominate digital signature message generated is the signing-for duration. As shown in FIG. 7, the data processing method for the innominate digital signature message specifically includes the following steps.

[0177] S701: if the signing-for duration information is the signing-for duration, generate a backflow innominate digital signature message and determine a message identifier and a message key of the backflow innominate digital signature message.

[0178] It should be noted that step S701 is similar to S202 in Embodiment 2, and is

not repeated here. In addition, value data of the backflow innominate digital signature message is zero, and signing-for duration information of the backflow innominate digital signature message is the unlimited signing-for duration identifier.

5 **[0179]** S702: establish and then store a corresponding relationship between the message identifier of the backflow innominate digital signature message and the message identifier of the second target innominate digital signature message.

10 **[0180]** S703: according to a current time and the signing-for duration information of the second target innominate digital signature message, if monitoring that the second target innominate digital signature message has not been signed for within a time limit, update status of the second target innominate digital signature message to be unavailable status, and update, according to the corresponding relationship between the message identifier of the backflow innominate digital signature message and the message identifier of the second target innominate digital signature message, the value data of the backflow innominate digital signature message to value data of the second target innominate digital signature message.

15 **[0181]** It should be noted that steps S702 and S703 are similar to steps S203 and S204 in Embodiment 2, and are not repeated here.

20 **[0182]** It should be noted that the value data of the second target innominate digital signature message may further be updated to zero.

25 **[0183]** It should be noted that the back end of the innominate digital signature message data management platform may further generate third signing-for record information according to the value data of the second target innominate digital signature message, and store the third signing-for record information in a change record data set of the value data of the backflow innominate digital signature message. The third signing-for record information is used to indicate value data transferred in from the second target innominate digital signature message, and the value data transferred in is equal to the value data of the second target innominate digital signature message. For the second target innominate digital signature message, corresponding record information may also be generated at this time, and stored in a change record data set

of the value data of the second target innominate digital signature message, to indicate value data transferred out to the backflow innominate digital signature message. The value data transferred out is equal to the value data of the second target innominate digital signature message.

5 **[0184]** In the data processing method for the innominate digital signature message provided by the embodiment, after generating the second target innominate digital signature message, if the signing-for duration information of the second target innominate digital signature message is the signing-for duration, the innominate digital signature message data management platform generates the backflow innominate digital signature message. Accordingly, in the case that through monitoring, the innominate digital signature message data management platform finds that the second target innominate digital signature message has not been signed for within the time limit, the innominate digital signature message data management platform updates the value data of the backflow innominate digital signature message. If monitoring that the second target innominate digital signature message has been signed for within the time limit, the innominate digital signature message data management platform updates the status of the backflow innominate digital signature message to be unavailable status. In this way, incidence of data anomalies is effectively reduced. Furthermore, this process does not involve a change of value data in the innominate digital signature message general data set, thus effectively improving the security.

15 **[0185]** FIG. 8 is a schematic flow diagram of Embodiment 8 of a data processing method for an innominate digital signature message provided by the present application. On the basis of the above-mentioned embodiments, this embodiment of the present application illustrates a case in which the innominate digital signature message data management platform performs signing-for of the innominate digital signature message to an existing innominate digital signature message. As shown in FIG. 8, the data processing method for the innominate digital signature message specifically includes the following steps.

25 **[0186]** S801: in response to an operation from a user for signing for an innominate

digital signature message to an existing message, obtain a message identifier of a to-be-signed-for innominate digital signature message and a message key of the to-be-signed-for innominate digital signature message and a message identifier of an innominate digital signature message for which transfer-in is to be done input by the user.

5 **[0187]** When getting an innominate digital signature message, a user can sign for it to an existing message on the innominate digital signature message data management platform. The user logs in to the front end of the innominate digital signature message data management platform and enters, on a signing-for interface, the message identifier and the message key of the to-be-signed-for innominate digital signature message and
10 the message identifier of the innominate digital signature message for which transfer-in is to be done.

[0188] In this step, the front end of the innominate digital signature message data management platform obtains, in response to the operation from the user for signing for the innominate digital signature message to the existing message, the message identifier
15 and the message key of the to-be-signed-for innominate digital signature message and the message identifier of the innominate digital signature message for which transfer-in is to be done input by the user, and then sends such information to the back end of the innominate digital signature message data management platform.

[0189] It should be noted that the user may directly input the message identifier and
20 the message key of the to-be-signed-for innominate digital signature message and the message identifier of the innominate digital signature message for which transfer-in is to be done through manual input, or may select from options displayed on the signing-for interface through a clicking operation to implement the input of the message identifier and the message key of the to-be-signed-for innominate digital signature
25 message and the message identifier of the innominate digital signature message for which transfer-in is to be done. The way for the user to input the message identifier and the message key of the to-be-signed-for innominate digital signature message and the message identifier of the innominate digital signature message for which transfer-in is to be done is not limited in embodiments of the present application and can be

determined according to an actual situation.

[0190] S802: verify, according to the message identifier of the to-be-signed-for innominate digital signature message, the message key of the to-be-signed-for innominate digital signature message and the message identifier of the innominate digital signature message for which transfer-in is to be done, both the to-be-signed-for innominate digital signature message and the innominate digital signature message for which transfer-in is to be done, to generate a second verification result.

[0191] In this step, after receiving the message identifier and the message key of the to-be-signed-for innominate digital signature message and the message identifier of the innominate digital signature message for which transfer-in is to be done, the back end of the innominate digital signature message data management platform first finds, according to the message identifier of the to-be-signed-for innominate digital signature message and the message identifier of the innominate digital signature message for which transfer-in is to be done, the to-be-signed-for innominate digital signature message and the innominate digital signature message for which transfer-in is to be done, and then verifies the to-be-signed-for innominate digital signature message and the innominate digital signature message for which transfer-in is to be done, to generate the second verification result.

[0192] Specifically, according to the message identifier of the to-be-signed-for innominate digital signature message and the message identifier of the innominate digital signature message for which transfer-in is to be done, the back end of the innominate digital signature message data management platform finds the to-be-signed-for innominate digital signature message and the innominate digital signature message for which transfer-in is to be done, and determines: whether or not the message identifier of the to-be-signed-for innominate digital signature message matches the message key of the to-be-signed-for innominate digital signature message, whether or not the status of the to-be-signed-for innominate digital signature message is available status, and whether or not value data of the to-be-signed-for innominate digital signature message is zero, and whether or not status of the innominate digital signature

message for which transfer-in is to be done is available status.

5 **[0193]** If the message identifier of the to-be-signed-for innominate digital signature message matches the message key of the to-be-signed-for innominate digital signature message and the status of the to-be-signed-for innominate digital signature message is the available status and the value data of the to-be-signed-for innominate digital signature message is not zero and the status of the innominate digital signature message for which transfer-in is to be done is the available status, the back end of the innominate digital signature message data management platform generates the second verification result that verification is passed.

10 **[0194]** If the message identifier of the to-be-signed-for innominate digital signature message does not match the message key of the to-be-signed-for innominate digital signature message and/or the status of the to-be-signed-for innominate digital signature message is unavailable status and/or the value data of the to-be-signed-for innominate digital signature message is zero and/or the status of the innominate digital signature message for which transfer-in is to be done is unavailable status, the back end of the innominate digital signature message data management platform generates the second verification result that verification is not passed.

15 **[0195]** S803: determine whether the second verification result is that verification is passed; if the second verification result is that verification is passed, execute step S804; if the second verification result is that verification is not passed, execute step S806.

20 **[0196]** In this step, after generating the second verification result, in order to determine whether a process of signing for the innominate digital signature message can be continued, the back end of the innominate digital signature message data management platform needs to judge whether the second verification result is that verification is passed.

25 **[0197]** S804: update, according to the value data of the to-be-signed-for innominate digital signature message, value data of the innominate digital signature message for which transfer-in is to be done.

[0198] S805: update, according to the message identifier of the to-be-signed-for

innominate digital signature message and the message key of the to-be-signed-for innominate digital signature message, status of the to-be-signed-for innominate digital signature message to be unavailable status.

[0199] In the above steps, if the back end of the innominate digital signature message data management platform judges that the second verification result is that verification is passed, it means that the process of signing for the innominate digital signature message can be continued. The back end of the innominate digital signature message data management platform then updates the value data of the innominate digital signature message for which transfer-in is to be done according to the value data of the to-be-signed-for innominate digital signature message, that is, uses a sum of the value data of the to-be-signed-for innominate digital signature message and the value data of the innominate digital signature message for which transfer-in is to be done, as updated value data of the innominate digital signature message for which transfer-in is to be done.

[0200] Accordingly, the back end of the innominate digital signature message data management platform can find the to-be-signed-for innominate digital signature message according to the message identifier of the to-be-signed-for innominate digital signature message and the message key of the to-be-signed-for innominate digital signature message, and gets permission to perform data processing for the to-be-signed-for innominate digital signature message, and updates the status of the to-be-signed-for innominate digital signature message to be unavailable status.

[0201] In addition, the value data of the to-be-signed-for innominate digital signature message may also be updated to zero.

[0202] It should be noted that the back end of the innominate digital signature message data management platform may further generate a signing-for result that signing-for is successful, and then send the signing-for result to the front end of the innominate digital signature message data management platform for display, so that the user can have a check.

[0203] It should be noted that the back end of the innominate digital signature

message data management platform may further generate third signing-for record information according to the value data of the to-be-signed-for innominate digital signature message, and store the third signing-for record information in a change record data set of the to-be-signed-for innominate digital signature message. The third signing-
5 for record information is used to indicate value data transferred out to the innominate digital signature message for which transfer-in is to be done, and the value data transferred out is equal to the value data of the to-be-signed-for innominate digital signature message.

[0204] According to the value data of the to-be-signed-for innominate digital
10 signature message, fourth signing-for record information is generated and stored in a change record data set of the innominate digital signature message for which transfer-in is to be done. The fourth signing-for record information is used to indicate value data transferred in from the to-be-signed-for innominate digital signature message. The value data transferred in is equal to the value data of the to-be-signed-for innominate
15 digital signature message.

[0205] S806: generate a signing-for result.

[0206] S807: display the signing-for result.

[0207] In the above steps, if the back end of the innominate digital signature message data management platform judges that the second verification result is that
20 verification is not passed, it means that the process of signing for the innominate digital signature message cannot be continued. The signing-for result that signing-for fails is generated and then sent to the front end of the innominate digital signature message data management platform for display, so that the user can have a check.

[0208] It should be noted that there may further be an incentive record data set in
25 the innominate digital signature message data management platform. During the signing-for operation, according to a preset signing-for incentive mode, signing-for incentive value data is determined and stored in the incentive record data set. A difference between the value data of the innominate digital signature message for which transfer-in is to be done and the signing-for incentive value data is used as updated

value data of the innominate digital signature message for which transfer-in is to be done, and record information is generated correspondingly and stored in the change record data set of the innominate digital signature message for which transfer-in is to be done. The record information is used to indicate value data transferred out to the
5 incentive record data set, and the value data transferred out is equal to the signing-for incentive value data.

[0209] It should be noted that determining, according to the preset signing-for incentive mode, the signing-for incentive value data may be as follows: using a product of the value data of the to-be-signed-for innominate digital signature message and a
10 preset ratio as the signing-for incentive value data, or, using preset signing-for incentive value data as the signing-for incentive value data, or, determining a signing-for value data threshold range corresponding to the value data of the to-be-signed-for innominate digital signature message, and then determining a preset ratio corresponding to the signing-for value data threshold range, and finally using a product of the value data of
15 the to-be-signed-for innominate digital signature message and the preset ratio as the signing-for incentive value data. The way of determining the signing-for incentive value data according to the preset data signing-for incentive mode is not limited in embodiments of the present application and can be determined according to an actual situation.

20 **[0210]** In the data processing method for the innominate digital signature message provided by the embodiment, signing-for of the innominate digital signature message, especially signing-for of the innominate digital signature message to an existing innominate digital signature message, can be implemented through the innominate digital signature message data management platform, without the information of the
25 recipient user. Furthermore, this process does not involve a change of value data in the innominate digital signature message general data set, thus effectively improving the security.

[0211] FIG. 9 is a schematic flow diagram of Embodiment 9 of a data processing method for an innominate digital signature message provided by the present application.

On the basis of the above-mentioned embodiments, this embodiment of the present application illustrates a case in which the innominate digital signature message data management platform splits the innominate digital signature message. As shown in FIG. 9, the data processing method for the innominate digital signature message specifically includes the following steps.

[0212] S901: in response to an operation from a user for splitting an innominate digital signature message, obtain an innominate digital signature message data management platform identity of the user and, a message identifier of a to-be-split innominate digital signature message, a message key of the to-be-split innominate digital signature message, a total number of split innominate digital signature messages, and value data of each of the split innominate digital signature messages and signing-for duration information of each of the split innominate digital signature messages input by the user.

[0213] The user can perform data splitting processing for the innominate digital signature message whose message identifier and message key are known to the user. The user logs in to the front end of the innominate digital signature message data management platform, and enters, on a splitting interface, the message identifier of the to-be-split innominate digital signature message and the message key of the to-be-split innominate digital signature message, the total number of the split innominate digital signature messages (innominate digital signature messages after splitting), and the value data and the signing-for duration information of each of the split innominate digital signature messages, and clicks a "Split" button.

[0214] In this step, the front end of the innominate digital signature message data management platform obtains, in response to the operation from the user for splitting the innominate digital signature message, the message identifier of the to-be-split innominate digital signature message and the message key of the to-be-split innominate digital signature message, the total number of the split innominate digital signature messages, and the value data and the signing-for duration information of each of the split innominate digital signature messages input by the user, and the innominate digital

signature message data management platform identity of the user, and sends such information to the back end of the innominate digital signature message data management platform.

5 **[0215]** S902: verify, according to the message identifier of the to-be-split innominate digital signature message and the message key of the to-be-split innominate digital signature message and the value data of each of the split innominate digital signature messages, the to-be-split innominate digital signature message to generate a third verification result.

10 **[0216]** In this step, after receiving the message identifier of the to-be-split innominate digital signature message and the message key of the to-be-split innominate digital signature message, the total number of the split innominate digital signature messages, the value data and the signing-for duration information of each of the split innominate digital signature messages and the innominate digital signature message data management platform identity of the user, the back end of the innominate digital signature message data management platform first verifies, according to the message identifier of the to-be-split innominate digital signature message and the value data of each of the split innominate digital signature messages, the to-be-split innominate digital signature message to generate the third verification result.

15 **[0217]** Specifically, according to the message identifier of the to-be-split innominate digital signature message, the back end of the innominate digital signature message data management platform finds the to-be-split innominate digital signature message, and determines: whether or not the message identifier of the to-be-split innominate digital signature message matches the message key of the to-be-split innominate digital signature message, and then whether or not status of the to-be-split innominate digital signature message is available status, whether or not value data of the to-be-split innominate digital signature message is zero, and whether or not a sum of value data of all the split innominate digital signature messages is greater than the value data of the to-be-split innominate digital signature message.

25 **[0218]** If the message identifier of the to-be-split innominate digital signature

message matches the message key of the to-be-split innominate digital signature message and the status of the to-be-split innominate digital signature message is the available status and the value data of the to-be-split innominate digital signature message is not zero and the sum of the value data of all the split innominate digital signature messages is less than or equal to the value data of the to-be-split innominate digital signature message, the back end of the innominate digital signature message data management platform generates the third verification result that verification is passed.

[0219] If the message identifier of the to-be-split innominate digital signature message does not match the message key of the to-be-split innominate digital signature message and/or the status of the to-be-split innominate digital signature message is the unavailable status and/or the value data of the to-be-split innominate digital signature message is zero and/or the sum of the value data of all the split innominate digital signature messages is greater than the value data of the to-be-split innominate digital signature message, the back end of the innominate digital signature message data management platform generates the third verification result that verification is not passed.

[0220] S903: judge whether the third verification result is that verification is passed; if the third verification result is that verification is passed, execute step S904; if the third verification result is that verification is not passed, execute step S910.

[0221] In this step, after generating the third verification result, in order to determine whether a process of splitting the innominate digital signature message can be continued, the back end of the innominate digital signature message data management platform needs to judge whether the third verification result is that verification is passed.

[0222] S904: generate, according to the total number of the split innominate digital signature messages and the value data and the signing-for duration information of each of the split innominate digital signature messages, the split innominate digital signature messages whose number is the total number, and determine a message identifier and a message key of each of the split innominate digital signature messages.

[0223] In the above steps, if the back end of the innominate digital signature message data management platform judges that the third verification result is that verification is passed, it means that the process of splitting the innominate digital signature message can be continued. Then the back end of the innominate digital signature message data management platform generates, according to the total number of the split innominate digital signature messages and the value data and the signing-for duration information of each of the split innominate digital signature messages, the split innominate digital signature messages whose number is the total number, and determines the message identifier and the message key of each of the split innominate digital signature messages. For each split innominate digital signature message, value data and signing-for duration information of the each split innominate digital signature message are respectively value data and signing-for duration information input by the user for the each split innominate digital signature message.

[0224] S905: judge whether the sum of the value data of all the split innominate digital signature messages is equal to the value data of the to-be-split innominate digital signature message; if the sum of the value data of all the split innominate digital signature messages is equal to the value data of the to-be-split innominate digital signature message, execute step S906; if the sum of the value data of all the split innominate digital signature messages is less than the value data of the to-be-split innominate digital signature message, then execute step S907.

[0225] In this step, after generating the split innominate digital signature messages, the back end of the innominate digital signature message data management platform also needs to process the to-be-split innominate digital signature message, and thus needs to judge whether the sum of the value data of all the split innominate digital signature messages is equal to the value data of the to-be-split innominate digital signature message. Because the third verification result is that verification is passed, it means that the sum of the value data of all the split innominate digital signature messages is less than or equal to the value data of the to-be-split innominate digital signature message, this leaves no room for the sum of the value data of all the split

innominate digital signature messages being greater than the value data of the to-be-split innominate digital signature message.

5 **[0226]** S906: update, according to the message identifier of the to-be-split innominate digital signature message and the message key of the to-be-split innominate digital signature message, the status of the to-be-split innominate digital signature message to be unavailable status.

10 **[0227]** In this step, if the sum of the value data of all the split innominate digital signature messages is equal to the value data of the to-be-split innominate digital signature message, it means that the to-be-split innominate digital signature message needs to be invalidated. The back end of the innominate digital signature message data management platform can find the to-be-split innominate digital signature message according to the message identifier of the to-be-split innominate digital signature message and the message key of the to-be-split innominate digital signature message, and gets permission to perform data processing for the to-be-split innominate digital signature message, and updates the status of the to-be-split innominate digital signature message to be unavailable status.

15 **[0228]** In addition, the value data of the to-be-split innominate digital signature message can also be updated to zero.

20 **[0229]** S907: determine a difference between the value data of the to-be-split innominate digital signature message and the sum of the value data of all the split innominate digital signature messages, as a first target difference.

25 **[0230]** S908: update, according to the message identifier of the to-be-split innominate digital signature message and the message key of the to-be-split innominate digital signature message, the value data of the to-be-split innominate digital signature message to the first target difference.

[0231] In the above steps, if the sum of the value data of all the split innominate digital signature messages is less than the value data of the to-be-split innominate digital signature message, it means that the to-be-split innominate digital signature message can still be used. The back end of the innominate digital signature message data

management platform determines the difference between the value data of the to-be-split innominate digital signature message and the sum of the value data of all the split innominate digital signature messages as the first target difference, and then finds the to-be-split innominate digital signature message according to the message identifier of the to-be-split innominate digital signature message and the message key of the to-be-split innominate digital signature message, and gets permission to perform data processing for the to-be-split innominate digital signature message, and updates the value data of the to-be-split innominate digital signature message to the first target difference.

5 [0232] It should be noted that, in the case where the sum of the value data of all the split innominate digital signature messages is less than or equal to the value data of the to-be-split innominate digital signature message, the back end of the innominate digital signature message data management platform may further generate a splitting result that splitting is successful, and then send the splitting result to the front end of the innominate digital signature message data management platform for display, so that the user can have a check.

15 [0233] It should be noted that, in the case where the sum of the value data of all the split innominate digital signature messages is less than or equal to the value data of the to-be-split innominate digital signature message, the back end of the innominate digital signature message data management platform may further generate first splitting record information according to the value data of each of the split innominate digital signature messages, and store the first splitting record information in a change record data set of the to-be-split innominate digital signature message. The first splitting record information includes sub-record information, where the number of pieces of the sub-record information is equal to the total number of the split innominate digital signature messages. Each piece of sub-record information corresponds to each split innominate digital signature message. Each piece of sub-record information is used to indicate value data transferred out to the corresponding split innominate digital signature message, and the value data transferred out is equal to the value data of the

corresponding split innominate digital signature message.

5 **[0234]** For each split innominate digital signature message, according to the value data of the split innominate digital signature message, second splitting record information is generated and stored in a change record data set of the split innominate digital signature message. The second splitting record information is used to indicate value data transferred in from the to-be-split innominate digital signature message, and the value data transferred in is equal to the value data of the split innominate digital signature message.

[0235] S909: generate a splitting result.

10 **[0236]** S910: display the splitting result.

[0237] In the above steps, if the back end of the innominate digital signature message data management platform judges that the third verification result is that verification is not passed, it means that the process of splitting the innominate digital signature message cannot be continued. The splitting result that splitting fails is
15 generated and then sent to the front end of the innominate digital signature message data management platform for display, so that the user can have a check.

[0238] It should be noted that there may further be an incentive record data set in the innominate digital signature message data management platform. During the splitting operation, according to a preset splitting incentive mode, splitting incentive
20 value data is determined and stored into the incentive record data set. Illustratively, if the value data of the to-be-split innominate digital signature message after the to-be-split innominate digital signature message is split is greater than or equal to the splitting incentive value data, a difference between the value data of the to-be-split innominate digital signature message after the to-be-split innominate digital signature message is
25 split and the splitting incentive value data is used as updated value data of the to-be-split innominate digital signature message, and record information is generated correspondingly and stored in the change record data set of the to-be-split innominate digital signature message. The record information is used to indicate value data transferred out to the incentive record data set, and the value data transferred out is

equal to the splitting incentive value data. If the value data of the to-be-split innominate digital signature message after the to-be-split innominate digital signature message is split is less than the splitting incentive value data, one split innominate digital signature message is determined from split innominate digital signature message(s) whose value data is greater than or equal to the splitting incentive value data. A difference between value data of the determined split innominate digital signature message and the splitting incentive value data is used as updated value data of the determined split innominate digital signature message, and record information is generated correspondingly and stored in a change record data set of the determined split innominate digital signature message. The record information is used to indicate value data transferred out to the incentive record set, and the value data transferred out is equal to the splitting incentive value data.

[0239] It should be noted that determining, according to the preset splitting incentive mode, the splitting incentive value data may be as follows: using a product of the sum of the value data of all the split innominate digital signature messages and a preset ratio as the splitting incentive value data, or, using preset splitting incentive value data as the splitting incentive value data, or, determining a splitting value data threshold range corresponding to the sum of the value data of all the split innominate digital signature messages, and then determining a preset ratio corresponding to the splitting value data threshold range, and finally using a product of the sum of the value data of all the split innominate digital signature messages and the preset ratio as the splitting incentive value data. The way of determining the splitting incentive value data according to the preset splitting incentive mode is not limited in embodiments of the present application and can be determined according to an actual situation.

[0240] In the data processing method for the innominate digital signature message provided by the embodiment, data processing for the splitting of the innominate digital signature message can be implemented through the innominate digital signature message data management platform, without the information of the recipient user. Furthermore, this process does not involve a change of value data in the innominate

digital signature message general data set, thus effectively improving the security.

[0241] FIG. 10 is a schematic flow diagram of Embodiment 10 of a data processing method for an innominate digital signature message provided by the present application. On the basis of the above-mentioned embodiments, this embodiment of the present application illustrates a case in which the innominate digital signature message data management platform generates a backflow innominate digital signature message if signing-for duration information of a split innominate digital signature message generated is the signing-for duration. As shown in FIG. 10, the data processing method for the innominate digital signature message specifically includes the following steps.

[0242] S1001: for each split innominate digital signature message, if signing-for duration information of the split innominate digital signature message is the signing-for duration, generate a backflow innominate digital signature message and determine a message identifier and a message key of the backflow innominate digital signature message.

[0243] It should be noted that step S1001 is similar to S202 in Embodiment 2, and is not repeated here. In addition, value data of the backflow innominate digital signature message is zero, and signing-for duration information of the backflow innominate digital signature message is the unlimited signing-for duration identifier.

[0244] S1002: establish and then store a corresponding relationship between the message identifier of the backflow innominate digital signature message and a message identifier of the split innominate digital signature message.

[0245] S1003: according to a current time and the signing-for duration information of the split innominate digital signature message, if monitoring that the split innominate digital signature message has not been signed for within a time limit, update status of the split innominate digital signature message to be unavailable status, and update, according to the corresponding relationship between the message identifier of the backflow innominate digital signature message and the message identifier of the split innominate digital signature message, the value data of the backflow innominate digital signature message to value data of the split innominate digital signature message.

[0246] It should be noted that steps S1002 and S1003 are similar to steps S203 and S204 in Embodiment 2, and are not repeated here.

[0247] It should be noted that the value data of the split innominate digital signature message may further be updated to zero.

5 **[0248]** It should be noted that the back end of the innominate digital signature message data management platform may further generate third splitting record information according to the value data of the split innominate digital signature message, and store the third splitting record information in a change record data set of the value data of the backflow innominate digital signature message. The third splitting record
10 information is used to indicate value data transferred in from the split innominate digital signature message, and the value data transferred in is equal to the value data of the split innominate digital signature message. For the split innominate digital signature message, corresponding record information may also be generated at this time, and stored in a change record data set of the value data of the split innominate digital
15 signature message, to indicate value data transferred out to the backflow innominate digital signature message. The value data transferred out is equal to the value data of the split innominate digital signature message.

[0249] In the data processing method for the innominate digital signature message provided by the embodiment, after generating a split innominate digital signature
20 message, if the signing-for duration information of the split innominate digital signature message is the signing-for duration, the innominate digital signature message data management platform generates the backflow innominate digital signature message. Accordingly, in the case that through monitoring, the innominate digital signature message data management platform finds that the split innominate digital signature
25 message has not been signed for within the time limit, the innominate digital signature message data management platform updates the value data of the backflow innominate digital signature message. If monitoring that the split innominate digital signature message has been signed for within the time limit, the innominate digital signature message data management platform updates the status of the backflow innominate

digital signature message to be unavailable status. In this way, incidence of data anomalies is effectively reduced. Furthermore, this process does not involve a change of value data in the innominate digital signature message general data set, thus effectively improving the security.

5 **[0250]** FIG. 11 is a schematic flow diagram of Embodiment 11 of a data processing method for an innominate digital signature message provided by the present application. On the basis of the above-mentioned embodiments, this embodiment of the present application illustrates a case in which the innominate digital signature message data management platform merges innominate digital signature messages into a new
10 innominate digital signature message. As shown in FIG. 11, the data processing method for the innominate digital signature message specifically includes the following steps.

[0251] S1101: in response to an operation from a user for merging innominate digital signature messages into a new message, obtain an innominate digital signature message data management platform identity of the user and, message identifiers of a
15 plurality of to-be-merged innominate digital signature messages and message keys of the plurality of to-be-merged innominate digital signature messages and signing-for duration information input by the user.

[0252] When getting a plurality of innominate digital signature messages, a user can merge them into a new message on the innominate digital signature message data
20 management platform. The user logs in to the front end of the innominate digital signature message data management platform and enters, on a merging interface, message identifiers of a plurality of to-be-merged innominate digital signature messages and message keys of the plurality of to-be-merged innominate digital signature messages and signing-for duration information.

25 **[0253]** In this step, the front end of the innominate digital signature message data management platform obtains, in response to the operation from the user for merging the innominate digital signature messages into the new message, the message identifiers of the plurality of to-be-merged innominate digital signature messages and the message keys of the plurality of to-be-merged innominate digital signature messages and the

signing-for duration information input by the user, and the innominate digital signature message data management platform identity of the user, and then sends such information to the back end of the innominate digital signature message data management platform.

5 **[0254]** It should be noted that the user may directly input the message identifiers of the plurality of to-be-merged innominate digital signature messages and the message keys of the plurality of to-be-merged innominate digital signature messages and the signing-for duration information through manual input, or may select from options displayed on the merging interface through a clicking operation to implement the input
10 of the message identifiers of the plurality of to-be-merged innominate digital signature messages and the message keys of the plurality of to-be-merged innominate digital signature messages and the signing-for duration information. The way for the user to input the message identifiers of the plurality of to-be-merged innominate digital signature messages and the message keys of the plurality of to-be-merged innominate
15 digital signature messages and the signing-for duration information is not limited in embodiments of the present application and can be determined according to an actual situation.

[0255] S1102: verify, according to the message identifiers of the plurality of to-be-merged innominate digital signature messages and the message keys of the plurality of
20 to-be-merged innominate digital signature messages, the plurality of to-be-merged innominate digital signature messages to generate a fourth verification result.

[0256] In this step, after receiving the message identifiers of the plurality of to-be-merged innominate digital signature messages and the message keys of the plurality of to-be-merged innominate digital signature messages, the signing-for duration
25 information and the innominate digital signature message data management platform identity of the user, the back end of the innominate digital signature message data management platform first verifies, according to the message identifiers of the plurality of to-be-merged innominate digital signature messages, the plurality of to-be-merged innominate digital signature messages to generate the fourth verification result.

[0257] Specifically, according to the message identifiers of the plurality of to-be-merged innominate digital signature messages, the back end of the innominate digital signature message data management platform finds the corresponding plurality of to-be-merged innominate digital signature messages, and determines: whether or not the message identifier of each to-be-merged innominate digital signature message matches the message key of the each to-be-merged innominate digital signature message, that is, for each to-be-merged innominate digital signature message, whether or not its message identifier and message key match, and then whether or not status of all to-be-merged innominate digital signature messages is available status.

[0258] If the message identifier of each to-be-merged innominate digital signature message matches the message key of each to-be-merged innominate digital signature message and the status of all the to-be-merged innominate digital signature messages is the available status, the back end of the innominate digital signature message data management platform generates the fourth verification result that verification is passed.

[0259] If there is at least one to-be-merged innominate digital signature message whose message identifier and message key do not match each other and/or there is at least one to-be-merged innominate digital signature message whose status is the unavailable status, the back end of the innominate digital signature message data management platform generates the fourth verification result that verification is not passed.

[0260] S1103: judge whether the fourth verification result is that verification is passed; if the fourth verification result is that verification is passed, execute step S1104; if the fourth verification result is that verification is not passed, execute step S1107.

[0261] In this step, after generating the fourth verification result, in order to determine whether a process of merging innominate digital signature messages can be continued, the back end of the innominate digital signature message data management platform needs to judge whether the fourth verification result is that verification is passed.

[0262] S1104: generate, according to the signing-for duration information input by

the user, a third target innominate digital signature message, and determine a message identifier and a message key of the third target innominate digital signature message.

[0263] S1105: update, according to the message identifiers of the plurality of to-be-merged innominate digital signature messages and the message keys of the plurality of to-be-merged innominate digital signature messages, status of the plurality of to-be-merged innominate digital signature messages to be unavailable status.

[0264] S1106: use a sum of value data of the plurality of to-be-merged innominate digital signature messages as value data of the third target innominate digital signature message.

[0265] In the above steps, if the back end of the innominate digital signature message data management platform judges that the fourth verification result is that verification is passed, it means that the process of merging innominate digital signature messages can be continued. The back end of the innominate digital signature message data management platform then generates the third target innominate digital signature message according to the signing-for duration information input by the user, that is, uses the signing-for duration information input by the user as signing-for duration information of the third target innominate digital signature message, and determines the message identifier and the message key of the third target innominate digital signature message.

[0266] Accordingly, for each to-be-merged innominate digital signature message, the back end of the innominate digital signature message data management platform can find a to-be-merged innominate digital signature message according to a message identifier and a message key of the to-be-merged innominate digital signature message, and gets permission to perform data processing for the to-be-merged innominate digital signature message, and updates status of the to-be-merged innominate digital signature message to be unavailable status. Besides, the back end of the innominate digital signature message data management platform can update the value data of the to-be-merged innominate digital signature message to zero.

[0267] For the third target innominate digital signature message, the sum of the

value data of the plurality of to-be-merged innominate digital signature messages is used as the value data of the third target innominate digital signature message.

[0268] It should be noted that the back end of the innominate digital signature message data management platform may further generate a merging result that merging
5 is successful, and then send the merging result to the front end of the innominate digital signature message data management platform for display, so that the user can have a check.

[0269] It should be noted that, for each to-be-merged innominate digital signature message, the back end of the innominate digital signature message data management
10 platform may further generate first merging record information according to value data of the to-be-merged innominate digital signature message, and store the first merging record information in a change record data set of the to-be-merged innominate digital signature message. The first merging record information is used to indicate value data transferred out to the third target innominate digital signature message, and the value
15 data transferred out is equal to the value data of the to-be-merged innominate digital signature message.

[0270] According to the value data of each of the to-be-merged innominate digital signature messages, second merging record information is generated and stored in a change record data set of the third target innominate digital signature message. The
20 second merging record information includes sub-record information, where the number of pieces of the sub-record information is equal to the total number of the to-be-merged innominate digital signature messages. Each piece of sub-record information corresponds to each to-be-merged innominate digital signature message. Each piece of sub-record information is used to indicate value data transferred in from a
25 corresponding to-be-merged innominate digital signature message, and the value data transferred in is equal to the value data of the corresponding to-be-merged innominate digital signature message.

[0271] S1107: generate a merging result.

[0272] S1108: display the merging result.

[0273] In the above steps, if the back end of the innominate digital signature message data management platform judges that the fourth verification result is that verification is not passed, it means that the process of merging innominate digital signature messages cannot be continued. The merging result that merging fails is generated and then sent to the front end of the innominate digital signature message data management platform for display, so that the user can have a check.

[0274] It should be noted that there may further be an incentive record data set in the innominate digital signature message data management platform. During the merging operation, according to a preset merging incentive mode, merging incentive value data is determined and stored into the incentive record data set. A difference between the value data of the third target innominate digital signature message and the merging incentive value data is used as updated value data of the third target innominate digital signature message, and record information is generated correspondingly and stored in the change record data set of the third target innominate digital signature message. The record information is used to indicate value data transferred out to the incentive record data set, and the value data transferred out is equal to the merging incentive value data.

[0275] It should be noted that determining, according to the preset merging incentive mode, the merging incentive value data may be as follows: using a product of the sum of the value data of all the to-be-merged innominate digital signature messages and a preset ratio as the merging incentive value data, or, using preset merging incentive value data as the merging incentive value data, or, determining a merging value data threshold range corresponding to the sum of the value data of all the to-be-merged innominate digital signature messages, and then determining a preset ratio corresponding to the merging value data threshold range, and finally using a product of the sum of the value data of all the to-be-merged innominate digital signature messages and the preset ratio as the merging incentive value data. The way of determining the merging incentive value data according to the preset merging incentive mode is not limited in embodiments of the present application and can be determined according to

an actual situation.

[0276] In the data processing method for the innominate digital signature message provided by the embodiment, merging of innominate digital signature messages, especially merging of innominate digital signature messages into a new innominate digital signature message, can be implemented through the innominate digital signature message data management platform, without the information of the recipient user. Furthermore, this process does not involve a change of value data in the innominate digital signature message general data set, thus effectively improving the security.

[0277] FIG. 12 is a schematic flow diagram of Embodiment 12 of a data processing method for an innominate digital signature message provided by the present application. On the basis of the above-mentioned embodiments, this embodiment of the present application illustrates a case in which the innominate digital signature message data management platform generates a backflow innominate digital signature message if the signing-for duration information of the third target innominate digital signature message generated is the signing-for duration. As shown in FIG. 12, the data processing method for the innominate digital signature message specifically includes the following steps.

[0278] S1201: if the signing-for duration information is the signing-for duration, generate a backflow innominate digital signature message and determine a message identifier and a message key of the backflow innominate digital signature message.

[0279] It should be noted that step S1201 is similar to S202 in Embodiment 2, and is not repeated here. In addition, value data of the backflow innominate digital signature message is zero, and signing-for duration information of the backflow innominate digital signature message is the unlimited signing-for duration identifier.

[0280] S1202: establish and then store a corresponding relationship between the message identifier of the backflow innominate digital signature message and the message identifier of the third target innominate digital signature message.

[0281] S1203: according to a current time and signing-for duration information of the third target innominate digital signature message, if monitoring that the third target

innominate digital signature message has not been signed for within a time limit, update status of the third target innominate digital signature message to be unavailable status, and update, according to the corresponding relationship between the message identifier of the backflow innominate digital signature message and the message identifier of the
5 third target innominate digital signature message, the value data of the backflow innominate digital signature message to the value data of the third target innominate digital signature message.

[0282] It should be noted that steps S1202 and S1203 are similar to steps S203 and S204 in Embodiment 2, and are not repeated here.

10 **[0283]** It should be noted that the value data of the third target innominate digital signature message may further be updated to zero.

[0284] It should be noted that the back end of the innominate digital signature message data management platform may further generate third merging record information according to the value data of the third target innominate digital signature
15 message, and store the third merging record information in a change record data set of the value data of the backflow innominate digital signature message. The third merging record information is used to indicate value data transferred in from the third target innominate digital signature message, and the value data transferred in is equal to the value data of the third target innominate digital signature message. For the third target
20 innominate digital signature message, corresponding record information may also be generated at this time, and stored in a change record data set of the value data of the third target innominate digital signature message, to indicate value data transferred out to the backflow innominate digital signature message. The value data transferred out is equal to the value data of the third target innominate digital signature message.

25 **[0285]** In the data processing method for the innominate digital signature message provided by the embodiment, after generating the third target innominate digital signature message, if the signing-for duration information of the third target innominate digital signature message is the signing-for duration, the innominate digital signature message data management platform generates the backflow innominate digital

signature message. Accordingly, in the case that through monitoring, the innominate digital signature message data management platform finds that the third target innominate digital signature message has not been signed for within the time limit, the innominate digital signature message data management platform updates the value data of the backflow innominate digital signature message. If monitoring that the third target innominate digital signature message has been signed for within the time limit, the innominate digital signature message data management platform updates the status of the backflow innominate digital signature message to be unavailable status. In this way, incidence of data anomalies is effectively reduced. Furthermore, this process does not involve a change of value data in the innominate digital signature message general data set, thus effectively improving the security.

[0286] FIG. 13 is a schematic flow diagram of Embodiment 13 of a data processing method for an innominate digital signature message provided by the present application. On the basis of the above-mentioned embodiments, this embodiment of the present application illustrates a case in which the innominate digital signature message data management platform merges innominate digital signature message(s) into an existing innominate digital signature message. As shown in FIG. 13, the data processing method for the innominate digital signature message specifically includes the following steps.

[0287] S1301: in response to an operation from a user for merging an innominate digital signature message into an existing message, obtain a message identifier of a fourth target innominate digital signature message and a message key of the fourth target innominate digital signature message and a message identifier of at least one to-be-merged innominate digital signature message and a message key of the at least one to-be-merged innominate digital signature message input by the user.

[0288] When getting a plurality of innominate digital signature messages, a user can merge them into an existing message on the innominate digital signature message data management platform. The user logs in to the front end of the innominate digital signature message data management platform and enters, on a merging interface, a message identifier of a fourth target innominate digital signature message and a

message key of the fourth target innominate digital signature message and a message identifier and a message key of at least one to-be-merged innominate digital signature message.

[0289] In this step, the front end of the innominate digital signature message data management platform obtains, in response to the operation from the user for merging the innominate digital signature message(s) into the existing message, the message identifier of the fourth target innominate digital signature message and the message key of the fourth target innominate digital signature message and the message identifier of the at least one to-be-merged innominate digital signature message and the message key of the at least one to-be-merged innominate digital signature message, and then sends such information to the back end of the innominate digital signature message data management platform.

[0290] It should be noted that the user may directly input the message identifier of the fourth target innominate digital signature message and the message key of the fourth target innominate digital signature message and the message identifier of the at least one to-be-merged innominate digital signature message and the message key of the at least one to-be-merged innominate digital signature message through manual input, or may select from options displayed on the merging interface through a clicking operation to implement the input of the message identifier of the fourth target innominate digital signature message and the message key of the fourth target innominate digital signature message and the message identifier of the at least one to-be-merged innominate digital signature message and the message key of the at least one to-be-merged innominate digital signature message. The way for the user to input the message identifier of the fourth target innominate digital signature message and the message key of the fourth target innominate digital signature message and the message identifier of the at least one to-be-merged innominate digital signature message and the message key of the at least one to-be-merged innominate digital signature message is not limited in embodiments of the present application and can be determined according to an actual situation.

[0291] S1302: verify, according to the message identifier of the fourth target innominate digital signature message and the message key of the fourth target innominate digital signature message and the message identifier of the at least one to-be-merged innominate digital signature message and the message key of the at least one to-be-merged innominate digital signature message, both the fourth target innominate digital signature message and the at least one to-be-merged innominate digital signature message to generate a fifth verification result.

[0292] In this step, after receiving the message identifier of the fourth target innominate digital signature message and the message key of the fourth target innominate digital signature message and the message identifier of the at least one to-be-merged innominate digital signature message and the message key of the at least one to-be-merged innominate digital signature message, the back end of the innominate digital signature message data management platform first finds, according to the message identifier of the fourth target innominate digital signature message and the message identifier of the at least one to-be-merged innominate digital signature message, the fourth target innominate digital signature message and the at least one to-be-merged innominate digital signature message, and verifies the fourth target innominate digital signature message and the at least one to-be-merged innominate digital signature message, to generate the fifth verification result.

[0293] Specifically, according to the message identifier of the fourth target innominate digital signature message and the message identifier of the at least one to-be-merged innominate digital signature message, the back end of the innominate digital signature message data management platform finds the fourth target innominate digital signature message and the at least one to-be-merged innominate digital signature message, and determines: whether or not the message identifier of the fourth target innominate digital signature message matches the message key of the fourth target innominate digital signature message, whether or not the message identifier of each to-be-merged innominate digital signature message matches the message key of the each to-be-merged innominate digital signature message, that is, for each of the at least one

to-be-merged innominate digital signature message, whether or not its message identifier and message key match each other, and then whether or not status of the fourth target innominate digital signature message is available status and whether or not status of all of the at least one to-be-merged innominate digital signature message is available status.

[0294] If the message identifier of the fourth target innominate digital signature message matches the message key of the fourth target innominate digital signature message and the message identifier of each to-be-merged innominate digital signature message matches the message key of the each to-be-merged innominate digital signature message and the status of the fourth target innominate digital signature message is the available status and the status of all of the at least one to-be-merged innominate digital signature message is the available status, the back end of the innominate digital signature message data management platform generates the fifth verification result that verification is passed.

[0295] If the message identifier of the fourth target innominate digital signature message does not match the message key of the fourth target innominate digital signature message and/or there is at least one to-be-merged innominate digital signature message whose message identifier and message key do not match each other and/or the status of the fourth target innominate digital signature message is unavailable status and/or there is at least one to-be-merged innominate digital signature message whose status is unavailable status, the back end of the innominate digital signature message data management platform generates the fifth verification result that verification is not passed.

[0296] S1303: judge whether the fifth verification result is that verification is passed; if the fifth verification result is that verification is passed, execute step S1304; if the fifth verification result is that verification is not passed, execute step S1306.

[0297] In this step, after generating the fifth verification result, in order to determine whether a process of merging innominate digital signature message(s) can be continued, the back end of the innominate digital signature message data management platform

needs to judge whether the fifth verification result is that verification is passed.

[0298] S1304: update, according to value data of the at least one to-be-merged innominate digital signature message, value data of the fourth target innominate digital signature message.

- 5 **[0299]** S1305: update, according to the message identifier of the at least one to-be-merged innominate digital signature message and the message key of the at least one to-be-merged innominate digital signature message, status of the at least one to-be-merged innominate digital signature message to be unavailable status.

[0300] In the above steps, if the back end of the innominate digital signature
10 message data management platform judges that the fifth verification result is that verification is passed, it means that the process of merging innominate digital signature messages can be continued. The back end of the innominate digital signature message data management platform then updates the value data of the fourth target innominate digital signature message according to the value data of the at least one to-be-merged
15 innominate digital signature message, that is, uses a sum of value data of all of the at least one to-be-merged innominate digital signature message and the value data of the fourth target innominate digital signature message as updated value data of the fourth target innominate digital signature message.

[0301] Accordingly, for each of the at least one to-be-merged innominate digital
20 signature message, the back end of the innominate digital signature message data management platform can find a to-be-merged innominate digital signature message according to a message identifier and a message key of the to-be-merged innominate digital signature message, and gets permission to perform data processing for the to-be-merged innominate digital signature message, and updates status of the to-be-merged
25 innominate digital signature message to be unavailable status. Besides, the back end of the innominate digital signature message data management platform can update the value data of the to-be-merged innominate digital signature message to zero.

[0302] It should be noted that the back end of the innominate digital signature message data management platform may further generate a merging result that merging

is successful, and then send the merging result to the front end of the innominate digital signature message data management platform for display, so that the user can have a check.

[0303] It should be noted that, for each to-be-merged innominate digital signature message of the at least one to-be-merged innominate digital signature message, the back end of the innominate digital signature message data management platform may further generate fourth merging record information according to value data of the to-be-merged innominate digital signature message, and store the fourth merging record information in a change record data set of the to-be-merged innominate digital signature message.

The fourth merging record information is used to indicate value data transferred out to the fourth target innominate digital signature message, and the value data transferred out is equal to the value data of the to-be-merged innominate digital signature message.

[0304] According to the value data of each of the at least one to-be-merged innominate digital signature message, fifth merging record information is generated and stored in a change record data set of the fourth target innominate digital signature message. The fifth merging record information includes sub-record information, where the number of pieces of the sub-record information is equal to the total number of the at least one to-be-merged innominate digital signature message. Each piece of sub-record information corresponds to each of the at least one to-be-merged innominate digital signature message. Each piece of sub-record information is used to indicate value data transferred in from a corresponding to-be-merged innominate digital signature message, and the value data transferred in is equal to the value data of the corresponding to-be-merged innominate digital signature message.

[0305] S1306: generate a merging result.

[0306] S1307: display the merging result.

[0307] In the above steps, if the back end of the innominate digital signature message data management platform judges that the fifth verification result is that verification is not passed, it means that the process of merging innominate digital signature message(s) cannot be continued. The merging result that merging fails is

generated and then sent to the front end of the innominate digital signature message data management platform for display, so that the user can have a check.

[0308] It should be noted that there may further be an incentive record data set in the innominate digital signature message data management platform. During the merging operation, according to a preset merging incentive mode, merging incentive value data is determined and stored into the incentive record data set. A difference between the value data of the fourth target innominate digital signature message and the merging incentive value data is used as updated value data of the fourth target innominate digital signature message, and record information is generated correspondingly and stored in the change record data set of the fourth target innominate digital signature message. The record information is used to indicate value data transferred out to the incentive record data set, and the value data transferred out is equal to the merging incentive value data.

[0309] It should be noted that determining, according to the preset merging incentive mode, the merging incentive value data may be as follows: using a product of the sum of the value data of all of the at least one to-be-merged innominate digital signature message and a preset ratio as the merging incentive value data, or, using preset merging incentive value data as the merging incentive value data, or, determining a merging value data threshold range corresponding to the sum of the value data of all of the at least one to-be-merged innominate digital signature message, and then determining a preset ratio corresponding to the merging value data threshold range, and finally using a product of the sum of the value data of all of the at least one to-be-merged innominate digital signature message and the preset ratio as the merging incentive value data. The way of determining the merging incentive value data according to the preset merging incentive mode is not limited in embodiments of the present application and can be determined according to an actual situation.

[0310] In the data processing method for the innominate digital signature message provided by the embodiment, merging of innominate digital signature messages, especially merging of innominate digital signature messages into an existing

innominate digital signature message, can be implemented through the innominate digital signature message data management platform, without the information of the recipient user. Furthermore, this process does not involve a change of value data in the innominate digital signature message general data set, thus effectively improving the security.

[0311] FIG. 14 is a schematic flow diagram of Embodiment 14 of a data processing method for an innominate digital signature message provided by the present application. On the basis of the above-mentioned embodiments, this embodiment of the present application illustrates a case in which the value data management platform sends, in response to a data transfer-out operation from a user, a data transfer-out request to the innominate digital signature message data management platform; the innominate digital signature message data management platform performs data transfer-out processing, and sends a data transfer request to the value data management platform; and the value data management platform transfers value data out from the innominate digital signature message general data set. As shown in FIG. 14, the data processing method for the innominate digital signature message specifically includes the following steps.

[0312] S1401: the value data management platform obtains, in response to a data transfer-out operation from a user, transfer-out value data, a message identifier of an innominate digital signature message for which transfer-out is to be done and a message key of the to-be-transferred-out innominate digital signature message, and a value data management platform identity input by the user.

[0313] To use an innominate digital signature message for data transfer-out processing, the user logs in to the value data management platform. At this time, the value data management platform that the user logged in to is a front end of the value data management platform. An interface for inputting data transfer-out information is displayed on an interface of the front end of the value data management platform. In this interface, the user enters the transfer-out value data, the message identifier of the innominate digital signature message for which transfer-out is to be done and the message key of the innominate digital signature message for which transfer-out is to be

done, and the value data management platform identity.

[0314] In this step, the front end of the value data management platform obtains, in response to a data transfer-out operation from the user, the transfer-out value data and the message identifier of the innominate digital signature message for which transfer-out is to be done and the message key of the innominate digital signature message for which transfer-out is to be done and the value data management platform identity input by the user, and sends such information to a back end of the value data management platform.

[0315] It should be noted that the user may directly input the transfer-out value data, the message identifier of the innominate digital signature message for which transfer-out is to be done and the message key of the innominate digital signature message for which transfer-out is to be done, and the value data management platform identity through manual input, or may select from options displayed on the interface for inputting data transfer-out information through a clicking operation to implement the input of the transfer-out value data, the message identifier of the innominate digital signature message for which transfer-out is to be done and the message key of the innominate digital signature message for which transfer-out is to be done, and the value data management platform identity. The way for the user to input the transfer-out value data, the message identifier of the innominate digital signature message for which transfer-out is to be done and the message key of the innominate digital signature message for which transfer-out is to be done, and the value data management platform identity is not limited in embodiments of the present application and can be determined according to an actual situation.

[0316] S1402: the value data management platform sends a data transfer-out request to the innominate digital signature message data management platform.

[0317] In this step, after receiving the transfer-out value data, the message identifier of the innominate digital signature message for which transfer-out is to be done and the message key of the innominate digital signature message for which transfer-out is to be done, and the value data management platform identity, the back end of the value data

management platform sends the data transfer-out request to the back end of innominate digital signature message data management platform since the data transfer-out processing of the innominate digital signature message is carried out on the innominate digital signature message data management platform. The data transfer-out request
5 includes the transfer-out value data, the message identifier of the innominate digital signature message for which transfer-out is to be done and the message key of the innominate digital signature message for which transfer-out is to be done, and the value data management platform identity.

[0318] S1403: after receiving the data transfer-out request sent by the value data
10 management platform, the innominate digital signature message data management platform verifies, according to the message identifier of the innominate digital signature message for which transfer-out is to be done and the message key of the innominate digital signature message for which transfer-out is to be done, the innominate digital signature message for which transfer-out is to be done to generate a sixth verification
15 result.

[0319] In this step, after the value data management platform sends the data transfer-out request to the innominate digital signature message data management platform, the back end of the innominate digital signature message data management platform can receive the data transfer-out request sent by the value data management
20 platform. The data transfer-out request includes the transfer-out value data, the message identifier of the innominate digital signature message for which transfer-out is to be done and the message key of the innominate digital signature message for which transfer-out is to be done, and the value data management platform identity.

[0320] Then, according to the message identifier of the innominate digital signature
25 message for which transfer-out is to be done and the message key of the innominate digital signature message for which transfer-out is to be done, the back end of the innominate digital signature message data management platform verifies the innominate digital signature message for which transfer-out is to be done to generate the sixth verification result.

[0321] Specifically, the back end of the innominate digital signature message data management platform finds, according to the message identifier of the innominate digital signature message for which transfer-out is to be done, the innominate digital signature message for which transfer-out is to be done, and determines: whether or not the message identifier of the innominate digital signature message for which transfer-out is to be done matches the message key of the innominate digital signature message for which transfer-out is to be done, whether or not the status of the innominate digital signature message for which transfer-out is to be done is available status, and whether or not the value data of the innominate digital signature message for which transfer-out is to be done is less than the transfer-out value data.

[0322] If the message identifier of the innominate digital signature message for which transfer-out is to be done matches the message key of the innominate digital signature message for which transfer-out is to be done and the status of the innominate digital signature message for which transfer-out is to be done is the available status and the value data of the innominate digital signature message for which transfer-out is to be done is greater than or equal to the transfer-out value data, the back end of the innominate digital signature message data management platform generates the sixth verification result that verification is passed.

[0323] If the message identifier of the innominate digital signature message for which transfer-out is to be done does not match the message key of the innominate digital signature message for which transfer-out is to be done and/or the status of the innominate digital signature message for which transfer-out is to be done is the unavailable status and/or the value data of the innominate digital signature message for which transfer-out is to be done is less than the transfer-out value data, the back end of the innominate digital signature message data management platform generates the sixth verification result that verification is not passed.

[0324] S1404: if the sixth verification result is that verification is passed, the innominate digital signature message data management platform sends a data transfer request to the value data management platform.

[0325] In this step, if the sixth verification result is verification is passed, it means that the data transfer-out process can be continued. Since processing of value data in the innominate digital signature message general data set is carried out on the value data management platform, the back end of the innominate digital signature message data management platform sends the data transfer request to the back end of the value data management platform. The data transfer request includes the transfer-out value data and the value data management platform identity.

[0326] It should be noted that if the sixth verification result is that the verification is not passed, it means that the data transfer-out process cannot be continued. The back end of the innominate digital signature message data management platform generates a data transfer-out result that data transfer-out fails, and then sends the data transfer-out result to the back end of the value data management platform. The back end of the value data management platform sends the data transfer-out result to the front end of the value data management platform for display, so that the user can have a check.

[0327] S1405: the innominate digital signature message data management platform judges whether value data of the innominate digital signature message for which transfer-out is to be done is greater than the transfer-out value data; if the value data of the innominate digital signature message for which transfer-out is to be done is greater than the transfer-out value data, execute step S1406; if value data of the innominate digital signature message for which transfer-out is to be done is equal to the transfer-out value data, execute step S1408.

[0328] In this step, the back-end of the innominate digital signature message data management platform continues the data transfer-out processing. Since the sixth verification result is that verification is passed, it means that the value data of the innominate digital signature message for which transfer-out is to be done is greater than or equal to the transfer-out value data. Therefore, in order to determine whether the innominate digital signature message for which transfer-out is to be done can continue to be used after the data is transferred out therefrom, it is also necessary to judge whether the value data of the innominate digital signature message for which transfer-

out is to be done is greater than the transfer-out value data.

[0329] S1406: the innominate digital signature message data management platform determines a difference between the value data of the innominate digital signature message for which transfer-out is to be done and the transfer-out value data, as a second
5 target difference.

[0330] S1407: the innominate digital signature message data management platform updates, according to the message identifier of the innominate digital signature message for which transfer-out is to be done and the message key of the innominate digital signature message for which transfer-out is to be done, the value data of the innominate
10 digital signature message for which transfer-out is to be done, to the second target difference.

[0331] In the above steps, if the value data of the innominate digital signature message for which transfer-out is to be done is greater than the transfer-out value data, it means that the innominate digital signature message for which transfer-out is to be
15 done can continue to be used after the data is transferred out therefrom. The back end of the innominate digital signature message data management platform determines the difference between the value data of the innominate digital signature message for which transfer-out is to be done and the transfer-out value data, as the second target difference, and then finds, according to the message identifier of the innominate digital signature
20 message for which transfer-out is to be done and the message key of the innominate digital signature message for which transfer-out is to be done, the innominate digital signature message for which transfer-out is to be done, and gets permission to perform data processing for the innominate digital signature message for which transfer-out is to be done, and updates the value data of the innominate digital signature message for
25 which transfer-out is to be done to the second target difference.

[0332] S1408: the innominate digital signature message data management platform updates, according to the message identifier of the innominate digital signature message for which transfer-out is to be done and the message key of the innominate digital signature message for which transfer-out is to be done, status of the innominate digital

signature message for which transfer-out is to be done to be unavailable status.

[0333] In this step, if the value data of the innominate digital signature message for which transfer-out is to be done is equal to the transfer-out value data, it means that the innominate digital signature message for which transfer-out is to be done cannot
5 continue to be used after the data is transferred out therefrom. The back end of the innominate digital signature message data management platform finds, according to the message identifier of the innominate digital signature message for which transfer-out is to be done and the message key of the innominate digital signature message for which transfer-out is to be done, the innominate digital signature message for which transfer-
10 out is to be done, and gets permission to perform data processing for the innominate digital signature message for which transfer-out is to be done, and updates the status of the innominate digital signature message for which transfer-out is to be done to be unavailable status, and in addition, may further update the value data of the innominate digital signature message for which transfer-out is to be done to zero.

[0334] It should be noted that, in the case where the value data of the innominate digital signature message for which transfer-out is to be done is greater than or equal to the transfer-out value data, the back end of the innominate digital signature message data management platform may further generate a data transfer-out result that data transfer-out is successful, and then send the data transfer-out result to the back end of
20 the value data management platform. The back end of the value data management platform sends the data transfer-out result to the front end of the value data management platform for display, so that the user can have a check.

[0335] It should be noted that, in the case where the value data of the innominate digital signature message for which transfer-out is to be done is greater than or equal to
25 the transfer-out value data, the back end of the innominate digital signature message data management platform may further generate data transfer-out record information according to the transfer-out value data, and store the data transfer-out record information in a change record data set of the innominate digital signature message for which transfer-out is to be done. The data transfer-out record information is used to

indicate value data transferred out, and the value data transferred out is equal to the transfer-out value data.

[0336] It should be noted that, with respect to an order of execution of steps S1404 and S1405-S1408, step S1404 may be executed first, and then steps S1405-S1408 are executed; or, steps S1405-S1408 may be executed first, and then step S1404 is executed; or, steps S1404 and S1405-S1408 are executed simultaneously. The order of execution of steps S1404 and S1405-S1408 is not limited in embodiments of the present application and can be determined according to an actual situation.

[0337] S1409: after receiving the data transfer request sent by the innominate digital signature message data management platform, the value data management platform transfers, according to the value data management platform identity and from the innominate digital signature message general data set corresponding to the innominate digital signature message data management platform, value data equal to the transfer-out value data into the identity data set corresponding to the value data management platform identity.

[0338] In this step, after the back end of the innominate digital signature message data management platform sends the data transfer request to the back end of the value data management platform, the back end of the value data management platform can receive the data transfer request. Then, according to the value data management platform identity included in the data transfer request, the back end of the value data management platform transfers, from the innominate digital signature message general data set corresponding to the innominate digital signature message data management platform, value data equal to the transfer-out value data into the identity data set corresponding to the value data management platform identity.

[0339] It should be noted that there may further be an incentive record data set in the innominate digital signature message data management platform. During the data transfer-out operation, according to a preset data transfer-out incentive mode, transfer-out incentive value data is determined and stored in the incentive record data set. Furthermore, if a source of preset incentive value data is the identity data set, the value

data management platform transfers, from the identity data set corresponding to the value data management platform identity, value data equal to the transfer-out incentive value data into the innominate digital signature message general data set corresponding to the innominate digital signature message management platform. If the source of the preset incentive value data is the innominate digital signature message, a difference between the value data of the innominate digital signature message for which transfer-out is to be done and the transfer-out incentive value data is used as updated value data of the innominate digital signature message for which transfer-out is to be done, and record information is generated correspondingly and stored in the change record data set of the innominate digital signature message for which transfer-out is to be done. The record information is used to indicate value data transferred out to the incentive record data set. The value data transferred out is equal to the transfer-out incentive value data.

[0340] It should be noted that determining, according to the preset data transfer-out incentive mode, the transfer-out incentive value data may be as follows: using a product of the transfer-out value data and a preset ratio as the transfer-out incentive value data, or, using preset transfer-out incentive value data as the transfer-out incentive value data, or, determining a transfer-out value data threshold range corresponding to the transfer-out value data, and then determining a preset ratio corresponding to the transfer-out value data threshold range, and finally using a product of the transfer-out value data and the preset ratio as the transfer-out incentive value data. The way of determining the transfer-out incentive value data according to the preset data transfer-out incentive mode is not limited in embodiments of the present application and can be determined according to an actual situation.

[0341] In the data processing method for the innominate digital signature message provided by the embodiment, the value data management platform sends, in response to a data transfer-out operation from the user, the data transfer-out request to the innominate digital signature message data management platform; the innominate digital signature message data management platform performs data transfer-out processing for the innominate digital signature message for which transfer-out is to be done, and sends

the data transfer request to the value data management platform; the value data management platform transfers, from the innominate digital signature message general data set corresponding to the innominate digital signature message data management platform, value data equal to the transfer-out value data into the identity data set
5 corresponding to the value data management platform identity. This solution implements the data transfer-out processing for the innominate digital signature message, even though there is no information of the recipient user in the innominate digital signature message for which transfer-out is to be done.

[0342] FIG. 15 is a schematic flow diagram of Embodiment 15 of a data processing
10 method for an innominate digital signature message provided by the present application. On the basis of the above-mentioned embodiments, this embodiment of the present application illustrates a case in which the innominate digital signature message data management platform, in response to a data transfer-out operation from a user, performs data transfer-out processing and sends a data transfer request to the value data
15 management platform, and the value data management platform transfers value data out from the innominate digital signature message general data set. As shown in FIG. 15, the data processing method for the innominate digital signature message specifically includes the following steps.

[0343] S1501: in response to a data transfer-out operation from a user, the
20 innominate digital signature message data management platform generates a data transfer-out request according to transfer-out value data, a message identifier of an innominate digital signature message for which transfer-out is to be done and a message key of the to-be-transferred-out innominate digital signature message, and a value data management platform identity input by the user.

25 **[0344]** The user logs in to the innominate digital signature message data management platform in order to transfer data out from an innominate digital signature message. At this time, the innominate digital signature message data management platform that the user logs in to is the front end of the innominate digital signature message data management platform. An interface for inputting data transfer-out

information is displayed on an interface of the front end of the innominate digital signature message data management platform. On this interface, the user enters the transfer-out value data, the message identifier of the innominate digital signature message for which transfer-out is to be done and the message key of the innominate digital signature message for which transfer-out is to be done, and the value data management platform identity.

[0345] In this step, the front end of the innominate digital signature message data management platform obtains, in response to the data transfer-out operation from the user, the transfer-out value data, the message identifier of the innominate digital signature message for which transfer-out is to be done and the message key of the innominate digital signature message for which transfer-out is to be done, and the value data management platform identity input by the user, and then sends such information to the back end of the innominate digital signature message data management platform.

[0346] It should be noted that the user may directly input the transfer-out value data, the message identifier of the innominate digital signature message for which transfer-out is to be done and the message key of the innominate digital signature message for which transfer-out is to be done, and the value data management platform identity through manual input, or may select from options displayed on the interface for inputting data transfer-out information through a clicking operation to implement the input of the transfer-out value data, the message identifier of the innominate digital signature message for which transfer-out is to be done and the message key of the innominate digital signature message for which transfer-out is to be done, and the value data management platform identity. The way for the user to input the transfer-out value data, the message identifier of the innominate digital signature message for which transfer-out is to be done and the message key of the innominate digital signature message for which transfer-out is to be done, and the value data management platform identity is not limited in embodiments of the present application and can be determined according to an actual situation.

[0347] S1502: the innominate digital signature message data management platform

verifies, according to the message identifier of the innominate digital signature message for which transfer-out is to be done and the message key of the innominate digital signature message for which transfer-out is to be done, the innominate digital signature message for which transfer-out is to be done to generate a sixth verification result.

- 5 **[0348]** It should be noted that step S1502 is similar to step S1403 in Embodiment 14, and details thereof are not repeated here.

[0349] S1503: the innominate digital signature message data management platform judges whether the sixth verification result is that verification is passed; if the sixth verification result is that verification is passed, execute step S1504; if the sixth
10 verification result is that verification is not passed, execute step S1510.

[0350] In this step, after generating the sixth verification result, in order to determine whether a process of transferring data out from the innominate digital signature message can be continued, the back end of the innominate digital signature message data management platform needs to judge whether the sixth verification result
15 is that verification is passed.

[0351] S1504: the innominate digital signature message data management platform sends a data transfer request to the value data management platform.

[0352] S1505: the innominate digital signature message data management platform judges whether value data of the innominate digital signature message for which
20 transfer-out is to be done is greater than the transfer-out value data; if the value data of the innominate digital signature message for which transfer-out is to be done is greater than the transfer-out value data, execute step S1506; if the value data of the innominate digital signature message for which transfer-out is to be done is equal to the transfer-out value data, execute step S1508.

25 **[0353]** S1506: the innominate digital signature message data management platform determines a difference between the value data of the innominate digital signature message for which transfer-out is to be done and the transfer-out value data, as a second target difference.

[0354] S1507: the innominate digital signature message data management platform

updates, according to the message identifier of the innominate digital signature message for which transfer-out is to be done and the message key of the innominate digital signature message for which transfer-out is to be done, the value data of the innominate digital signature message for which transfer-out is to be done, to the second target
5 difference.

[0355] S1508: the innominate digital signature message data management platform updates, according to the message identifier of the innominate digital signature message for which transfer-out is to be done and the message key of the innominate digital signature message for which transfer-out is to be done, status of the innominate digital
10 signature message for which transfer-out is to be done to be unavailable status.

[0356] It should be noted that steps S1504 to S1508 are similar to steps S1404 to S1408 in Embodiment 14, and details thereof are not repeated here.

[0357] It should be noted that, with respect to an order of execution of steps S1504 and S1505- S1508, step S1504 may be executed first, and then steps S1505-S1508 are
15 executed; or, steps S1505-S1508 may be executed first, and then step S1504 is executed; or, steps S1504 and S1505- S1508 may be executed simultaneously. The order of execution of steps S1504 and S1505- S1508 is not limited in embodiments of the present application and can be determined according to an actual situation.

[0358] It should be noted that, in the case where the value data of the innominate
20 digital signature message for which transfer-out is to be done is greater than or equal to the transfer-out value data, the back end of the innominate digital signature message data management platform may further generate a data transfer-out result that data transfer-out is successful, and then send the data transfer-out result to the front end of the innominate digital signature message data management platform for display, so that
25 the user can have a check.

[0359] S1509: after receiving the data transfer request sent by the innominate digital signature message data management platform, the value data management platform transfers, according to the value data management platform identity and from the innominate digital signature message general data set corresponding to the

innominate digital signature message data management platform, value data equal to the transfer-out value data into the identity data set corresponding to the value data management platform identity.

5 **[0360]** It should be noted that step S1509 is similar to step S1409 in Embodiment 14, and details thereof are not repeated here.

[0361] S1510: the innominate digital signature message data management platform generates a data transfer-out result.

[0362] S1511: the innominate digital signature message data management platform displays the data transfer-out result.

10 **[0363]** In the above steps, if the sixth verification result is that verification is not passed, it means that the process of transferring data out from the innominate digital signature message cannot be continued. The back end of the innominate digital signature message data management platform generates the data transfer-out result that data transfer-out fails and then sends the data transfer-out result to the front end of the
15 innominate digital signature message data management platform for display, so that the user can have a check.

[0364] In the data processing method for the innominate digital signature message provided by the embodiment, the innominate digital signature message data management platform performs, in response to a data transfer-out operation from the
20 user, data transfer-out processing for the innominate digital signature message from which the transfer-out value data is to be transferred out, and sends the data transfer request to the value data management platform. The value data management platform transfers, from the innominate digital signature message general data set corresponding to the innominate digital signature message data management platform, value data
25 equal to the transfer-out value data into the identity data set corresponding to the value data management platform identity. This solution implements the data transfer-out processing for the innominate digital signature message, even though there is no information of the recipient user in the innominate digital signature message for which transfer-out is to be done.

[0365] In the following, other aspects of the value data management platform and the innominate digital signature message data management platform provided by the present application are described.

[0366] The value data management platform has an authority to transfer value data in and out between different identity data sets. The innominate digital signature message data management platform has no authority to transfer value data in and out between different identity data sets.

[0367] One innominate digital signature message data management platform can be linked to multiple value data management platforms.

[0368] The value data in the present application may be monetary value, or a value share of valuable assets such as an artwork, a real estate, securities, etc., which is not limited in embodiments of the present application, and may be determined according to an actual situation.

[0369] For each type of value data, there is a corresponding innominate digital signature message data management platform for data processing.

[0370] For the incentive record data set, the user may further perform extraction operations. The user logs in to the front end of the value data management platform or the front end of the innominate digital signature message data management platform, and inputs extracted value data and a value data management platform identity. The front end of the value data management platform or the front end of the innominate digital signature message data management platform generates an extraction request. The extraction request includes the extracted value data and the value data management platform identity. If it is the front end of the value data management platform that the user logs in to, the front end of the value data management platform sends the extraction request to the back end of the value data management platform, and the back end of the value data management platform then sends the extraction request to the back end of the innominate digital signature message data management platform. If it is the front end of the innominate digital signature message data management platform that the user logs in to, the front end of the innominate digital signature message data management

platform sends the extraction request to the back end of the innominate digital signature message data management platform.

[0371] The back end of the innominate digital signature message data management platform uses a difference between value data of the incentive record data set and the extracted value data, as updated value data of the incentive record data set, and then sends an extraction instruction to the back end of the value data management platform. The extraction instruction includes the extracted value data and the value data management platform identity. The back end of the value data management platform transfers, from the innominate digital signature message general data set corresponding to the innominate digital signature message data management platform, value data equal to the extracted value data into the identity data set corresponding to the value data management platform identity.

[0372] If the user has only a message key of an innominate digital signature message and has no corresponding message identifier, a message identifier can be restored through the innominate digital signature message data management platform. The user logs in to the front end of the innominate digital signature message data management platform and inputs the message key. The front end of the innominate digital signature message data management platform sends the message key to the back end of the innominate digital signature message data management platform. The back end of the innominate digital signature message data management platform performs hash calculation according to the message key to obtain the message identifier, and returns the message identifier to the front end of the innominate digital signature message data management platform for display, so that the user can have a check.

[0373] The innominate digital signature message may be present in a form of a picture, a two-dimensional code, a barcode, a message identifier, etc. Forms of the innominate digital signature message are not limited in embodiments of the present application, and can be selected according to an actual situation.

[0374] With respect to types of the innominate digital signature message, the first target innominate digital signature message generated during data transfer-in

processing performed by the innominate digital signature message data management platform may be classified as an initial message; the backflow innominate digital signature message, the second target innominate digital signature message generated during data signing-for processing performed by the innominate digital signature message data management platform, the split innominate digital signature messages generated during data splitting processing performed by the innominate digital signature message data management platform, and the third target innominate digital signature message generated during data merging processing performed by the innominate digital signature message data management platform may be classified as secondary messages.

[0375] In the data processing method for the innominate digital signature message provided in the embodiments, data processing for the innominate digital signature message can be implemented without the information of the recipient user, and this is applicable to more scenarios and improves the user experience.

[0376] The following are apparatus embodiments of the present application, which can be used to implement the method embodiments of the present application. For details not disclosed in the apparatus embodiments of the present application, please refer to the method embodiments of the present application correspondingly.

[0377] FIG. 16 is a schematic structural diagram of Embodiment 1 of a data processing apparatus for an innominate digital signature message provided by the present application. As shown in FIG. 16, a data processing apparatus 160 for the innominate digital signature message includes:

a communicating module 161, configured to receive a data transfer-in request sent by a value data management platform, where the data transfer-in request includes a transfer-in data flow direction identifier and transfer-in value data, and the transfer-in data flow direction identifier is an innominate digital signature message data management platform identity or a message identifier of an innominate digital signature message for which transfer-in is to be done; and

a processing module 162, configured to:

generate a first target innominate digital signature message and determine a message identifier and a message key of the first target innominate digital signature message, if the transfer-in data flow direction identifier is the innominate digital signature message data management platform identity; and

5 determine the transfer-in value data as value data of the first target innominate digital signature message.

[0378] Furthermore, the processing module 162 is further configured to:

 determine, according to the message identifier of the innominate digital signature message for which transfer-in is to be done, whether or not status of the
10 innominate digital signature message for which transfer-in is to be done is available status, if the transfer-in data flow direction identifier is the message identifier of the innominate digital signature message for which transfer-in is to be done; and

 update, according to the transfer-in value data, value data of the innominate digital signature message for which transfer-in is to be done, if the status of the
15 innominate digital signature message for which transfer-in is to be done is the available status.

[0379] Furthermore, the processing module 162 is specifically configured to:

 use the signing-for duration information as signing-for duration information of the first target innominate digital signature message;

20 generate a backflow innominate digital signature message and determine a message identifier and a message key of the backflow innominate digital signature message, if the signing-for duration information is the signing-for duration, where value data of the backflow innominate digital signature message is zero, and signing-for duration information of the backflow innominate digital signature message is the
25 unlimited signing-for duration identifier;

 establish and then store a corresponding relationship between the message identifier of the backflow innominate digital signature message and the message identifier of the first target innominate digital signature message; and

 according to a current time and the signing-for duration information of the

first target innominate digital signature message, if monitoring that the first target innominate digital signature message has not been signed for within a time limit, update status of the first target innominate digital signature message to be unavailable status, and update, according to the corresponding relationship between the message identifier
5 of the backflow innominate digital signature message and the message identifier of the first target innominate digital signature message, the value data of the backflow innominate digital signature message to the value data of the first target innominate digital signature message.

[0380] The data processing apparatus 160 for the innominate digital signature
10 message may further include an obtaining module 163 configured to obtain, in response to an operation from a user for retrieving an innominate digital signature message, a message identifier of a to-be-retrieved innominate digital signature message input by the user;

the processing module 162 is further configured to obtain a retrieval result
15 according to the message identifier, where the retrieval result includes one or more of status of the to-be-retrieved innominate digital signature message, value data of the to-be-retrieved innominate digital signature message, signing-for duration information of the to-be-retrieved innominate digital signature message, and a change record data set of the to-be-retrieved innominate digital signature message; and

20 the data processing apparatus 160 for the innominate digital signature message may further include a displaying module 164 configured to display the retrieval result.

[0381] Furthermore, the obtaining module 163 is further configured to obtain, in response to an operation from a user for signing for an innominate digital signature
25 message to a new message, an innominate digital signature message data management platform identity of the user and, a message identifier of a to-be-signed-for innominate digital signature message and a message key of the to-be-signed-for innominate digital signature message and signing-for duration information input by the user; and

furthermore, the processing module 162 is further configured to:

verify, according to the message identifier of the to-be-signed-for innominate digital signature message and the message key of the to-be-signed-for innominate digital signature message, the to-be-signed-for innominate digital signature message to generate a first verification result;

- 5 if the first verification result is that verification is passed, generate, according to the signing-for duration information input by the user, a second target innominate digital signature message, and determine a message identifier and a message key of the second target innominate digital signature message;

- update, according to the message identifier of the to-be-signed-for
10 innominate digital signature message and the message key of the to-be-signed-for innominate digital signature message, status of the to-be-signed-for innominate digital signature message to be unavailable status; and

 use value data of the to-be-signed-for innominate digital signature message as value data of the second target innominate digital signature message.

- 15 **[0382]** Furthermore, the processing module 162 is further configured to:

- determine whether or not the message identifier of the to-be-signed-for innominate digital signature message matches the message key of the to-be-signed-for innominate digital signature message; and determine, according to the message identifier of the to-be-signed-for innominate digital signature message, whether or not
20 the status of the to-be-signed-for innominate digital signature message is available status, and whether or not the value data of the to-be-signed-for innominate digital signature message is zero;

- generate the first verification result that verification is passed, if the message identifier of the to-be-signed-for innominate digital signature message matches the
25 message key of the to-be-signed-for innominate digital signature message and the status of the to-be-signed-for innominate digital signature message is the available status and the value data of the to-be-signed-for innominate digital signature message is not zero;
and

 generate the first verification result that verification is not passed, if the

message identifier of the to-be-signed-for innominate digital signature message does not match the message key of the to-be-signed-for innominate digital signature message and/or the status of the to-be-signed-for innominate digital signature message is unavailable status and/or the value data of the to-be-signed-for innominate digital signature message is zero.

[0383] Furthermore, the obtaining module 163 is further configured to obtain, in response to an operation from a user for signing for an innominate digital signature message to an existing message, a message identifier of a to-be-signed-for innominate digital signature message and a message key of the to-be-signed-for innominate digital signature message and a message identifier of an innominate digital signature message for which transfer-in is to be done input by the user; and

the processing module 162 is further configured to:

verify, according to the message identifier of the to-be-signed-for innominate digital signature message, the message key of the to-be-signed-for innominate digital signature message and the message identifier of the innominate digital signature message for which transfer-in is to be done, both the to-be-signed-for innominate digital signature message and the innominate digital signature message for which transfer-in is to be done, to generate a second verification result;

if the second verification result is that verification is passed, update, according to value data of the to-be-signed-for innominate digital signature message, value data of the innominate digital signature message for which transfer-in is to be done; and

update, according to the message identifier of the to-be-signed-for innominate digital signature message and the message key of the to-be-signed-for innominate digital signature message, status of the to-be-signed-for innominate digital signature message to be unavailable status.

[0384] Furthermore, the processing module 162 is further configured to:

determine whether or not the message identifier of the to-be-signed-for innominate digital signature message matches the message key of the to-be-signed-for

innominate digital signature message; and determine, according to the message identifier of the to-be-signed-for innominate digital signature message and the message identifier of the innominate digital signature message for which transfer-in is to be done, whether or not the status of the to-be-signed-for innominate digital signature message
5 is available status, whether or not the value data of the to-be-signed-for innominate digital signature message is zero, and whether or not status of the innominate digital signature message for which transfer-in is to be done is available status;

generate the second verification result that verification is passed, if the message identifier of the to-be-signed-for innominate digital signature message
10 matches the message key of the to-be-signed-for innominate digital signature message and the status of the to-be-signed-for innominate digital signature message is the available status and the value data of the to-be-signed-for innominate digital signature message is not zero and the status of the innominate digital signature message for which transfer-in is to be done is the available status; and

15 generate the second verification result that verification is not passed, if the message identifier of the to-be-signed-for innominate digital signature message does not match the message key of the to-be-signed-for innominate digital signature message and/or the status of the to-be-signed-for innominate digital signature message is unavailable status and/or the value data of the to-be-signed-for innominate digital
20 signature message is zero and/or the status of the innominate digital signature message for which transfer-in is to be done is unavailable status.

[0385] Furthermore, the obtaining module 163 is further configured to obtain, in response to an operation from a user for splitting an innominate digital signature message, an innominate digital signature message data management platform identity
25 of the user and, a message identifier of a to-be-split innominate digital signature message and a message key of the to-be-split innominate digital signature message, a total number of split innominate digital signature messages, and value data of each of the split innominate digital signature messages and signing-for duration information of each of the split innominate digital signature messages input by the user; and

the processing module 162 is further configured to:

verify, according to the message identifier of the to-be-split innominate digital signature message and the message key of the to-be-split innominate digital signature message and the value data of each of the split innominate digital signature messages, the to-be-split innominate digital signature message to generate a third verification result;

if the third verification result is that verification is passed, generate, according to the total number of the split innominate digital signature messages and the value data and the signing-for duration information of each of the split innominate digital signature messages, the split innominate digital signature messages whose number is the total number, and determine a message identifier and a message key of each of the split innominate digital signature messages;

if a sum of value data of all the split innominate digital signature messages is equal to value data of the to-be-split innominate digital signature message, update, according to the message identifier of the to-be-split innominate digital signature message and the message key of the to-be-split innominate digital signature message, status of the to-be-split innominate digital signature message to be unavailable status;

if the sum of the value data of all the split innominate digital signature messages is less than the value data of the to-be-split innominate digital signature message, determine a difference between the value data of the to-be-split innominate digital signature message and the sum of the value data of all the split innominate digital signature messages, as a first target difference; and

update, according to the message identifier of the to-be-split innominate digital signature message and the message key of the to-be-split innominate digital signature message, the value data of the to-be-split innominate digital signature message to the first target difference.

[0386] Furthermore, the processing module 162 is further configured to:

determine whether or not the message identifier of the to-be-split innominate digital signature message matches the message key of the to-be-split

innominate digital signature message; and determine, according to the message identifier of the to-be-split innominate digital signature message and the value data of each of the split innominate digital signature messages, whether or not the status of the to-be-split innominate digital signature message is available status, whether or not the value data of the to-be-split innominate digital signature message is zero, and whether or not the sum of the value data of all the split innominate digital signature messages is greater than the value data of the to-be-split innominate digital signature message;

generate the third verification result that verification is passed, if the message identifier of the to-be-split innominate digital signature message matches the message key of the to-be-split innominate digital signature message and the status of the to-be-split innominate digital signature message is the available status and the value data of the to-be-split innominate digital signature message is not zero and the sum of the value data of all the split innominate digital signature messages is less than or equal to the value data of the to-be-split innominate digital signature message; and

generate the third verification result that verification is not passed, if the message identifier of the to-be-split innominate digital signature message does not match the message key of the to-be-split innominate digital signature message and/or the status of the to-be-split innominate digital signature message is the unavailable status and/or the value data of the to-be-split innominate digital signature message is zero and/or the sum of the value data of all the split innominate digital signature messages is greater than the value data of the to-be-split innominate digital signature message.

[0387] Furthermore, the processing module 162 is further configured to:

for each of the split innominate digital signature messages,

if signing-for duration information of a split innominate digital signature message is a signing-for duration, generate a backflow innominate digital signature message and determine a message identifier and a message key of the backflow innominate digital signature message, where value data of the backflow innominate digital signature message is zero, and signing-for duration information of the backflow

innominate digital signature message is an unlimited signing-for duration identifier;

establish and then store a corresponding relationship between the message identifier of the backflow innominate digital signature message and the message identifier of the split innominate digital signature message; and

5 according to a current time and the signing-for duration information of the split innominate digital signature message, if monitoring that the split innominate digital signature message has not been signed for within a time limit, update status of the split innominate digital signature message to be unavailable status, and update, according to the corresponding relationship between the message identifier of the backflow innominate digital signature message and the message identifier of the split
10 innominate digital signature message, the value data of the backflow innominate digital signature message to value data of the split innominate digital signature message.

[0388] Furthermore, the obtaining module 163 is further configured to obtain, in response to an operation from a user for merging innominate digital signature messages
15 into a new message, an innominate digital signature message data management platform identity of the user and, message identifiers of a plurality of to-be-merged innominate digital signature messages and message keys of the plurality of to-be-merged innominate digital signature messages and signing-for duration information input by the user; and

20 the processing module 162 is further configured to:

verify, according to the message identifiers of the plurality of to-be-merged innominate digital signature messages and the message keys of the plurality of to-be-merged innominate digital signature messages, the plurality of to-be-merged innominate digital signature messages to generate a fourth verification result;

25 if the fourth verification result is that verification is passed, generate, according to the signing-for duration information input by the user, a third target innominate digital signature message, and determine a message identifier and a message key of the third target innominate digital signature message;

update, according to the message identifiers of the plurality of to-be-merged

innominate digital signature messages and the message keys of the plurality of to-be-merged innominate digital signature messages, status of the plurality of to-be-merged innominate digital signature messages to be unavailable status; and

5 use a sum of value data of the plurality of to-be-merged innominate digital signature messages as value data of the third target innominate digital signature message.

[0389] Furthermore, the processing module 162 is further configured to:

10 determine whether or not a message identifier of each to-be-merged innominate digital signature message matches a message key of each to-be-merged innominate digital signature message; and determine, according to the message identifiers of the plurality of to-be-merged innominate digital signature messages, whether or not the status of all the to-be-merged innominate digital signature messages is available status;

15 generate the fourth verification result that verification is passed, if the message identifier of each to-be-merged innominate digital signature message matches the message key of each to-be-merged innominate digital signature message and the status of all the to-be-merged innominate digital signature messages is the available status; and

20 generate the fourth verification result that verification is not passed, if there is at least one to-be-merged innominate digital signature message whose message identifier and message key do not match each other and/or there is at least one to-be-merged innominate digital signature message whose status is the unavailable status.

[0390] Furthermore, the processing module 162 is further configured to:

25 generate a backflow innominate digital signature message and determine a message identifier and a message key of the backflow innominate digital signature message, if the signing-for duration information is a signing-for duration, where value data of the backflow innominate digital signature message is zero, and signing-for duration information of the backflow innominate digital signature message is an unlimited signing-for duration identifier;

establish and then store a corresponding relationship between the message identifier of the backflow innominate digital signature message and the message identifier of the third target innominate digital signature message; and

5 according to a current time and signing-for duration information of the third target innominate digital signature message, if monitoring that the third target innominate digital signature message has not been signed for within a time limit, update status of the third target innominate digital signature message to be unavailable status, and update, according to the corresponding relationship between the message identifier of the backflow innominate digital signature message and the message identifier of the
10 third target innominate digital signature message, the value data of the backflow innominate digital signature message to the value data of the third target innominate digital signature message.

[0391] Furthermore, the obtaining module 163 is further configured to obtain, in response to an operation from a user for merging an innominate digital signature
15 message into an existing message, a message identifier of a fourth target innominate digital signature message and a message key of the fourth target innominate digital signature message and a message identifier of at least one to-be-merged innominate digital signature message and a message key of the at least one to-be-merged innominate digital signature message input by the user; and

20 the processing module 162 is further configured to:

 verify, according to the message identifier of the fourth target innominate digital signature message and the message key of the fourth target innominate digital signature message and the message identifier of the at least one to-be-merged innominate digital signature message and the message key of the at least one to-be-merged innominate digital signature message, both the fourth target innominate digital
25 signature message and the at least one to-be-merged innominate digital signature message to generate a fifth verification result;

 if the fifth verification result is that verification is passed, update, according to value data of the at least one to-be-merged innominate digital signature message,

value data of the fourth target innominate digital signature message; and

update, according to the message identifier of the at least one to-be-merged innominate digital signature message and the message key of the at least one to-be-merged innominate digital signature message, status of the at least one to-be-merged innominate digital signature message to be unavailable status.

[0392] Furthermore, the processing module 162 is further configured to:

determine whether or not the message identifier of the fourth target innominate digital signature message matches the message key of the fourth target innominate digital signature message and whether or not the message identifier of each to-be-merged innominate digital signature message matches the message key of the each to-be-merged innominate digital signature message; and determine, according to the message identifier of the fourth target innominate digital signature message and the message identifier of the at least one to-be-merged innominate digital signature message, whether or not status of the fourth target innominate digital signature message is available status and whether or not status of all of the at least one to-be-merged innominate digital signature message is available status;

generate the fifth verification result that verification is passed, if the message identifier of the fourth target innominate digital signature message matches the message key of the fourth target innominate digital signature message and the message identifier of each to-be-merged innominate digital signature message matches the message key of the each to-be-merged innominate digital signature message and the status of the fourth target innominate digital signature message is the available status and the status of all of the at least one to-be-merged innominate digital signature message is the available status; and

generate the fifth verification result that verification is not passed, if the message identifier of the fourth target innominate digital signature message does not match the message key of the fourth target innominate digital signature message and/or there is at least one to-be-merged innominate digital signature message whose message identifier and message key do not match each other and/or the status of the fourth target

innominate digital signature message is unavailable status and/or there is at least one to-be-merged innominate digital signature message whose status is unavailable status.

[0393] Furthermore, the obtaining module 163 is further configured to obtain a data transfer-out request, where the data transfer-out request includes transfer-out value data, a message identifier of an innominate digital signature message for which transfer-out is to be done and a message key of the to-be-transferred-out innominate digital signature message, and a value data management platform identity, and the data transfer-out request is sent by the value data management platform, or, the data transfer-out request is generated, in response to a data transfer-out operation from a user, according to the transfer-out value data, the value data management platform identity, the message identifier of the innominate digital signature message for which transfer-out is to be done and the message key of the innominate digital signature message for which transfer-out is to be done input by the user; and

the processing module 162 is further configured to:

verify, according to the message identifier of the innominate digital signature message for which transfer-out is to be done and the message key of the innominate digital signature message for which transfer-out is to be done, the innominate digital signature message for which transfer-out is to be done to generate a sixth verification result;

if the sixth verification result is that verification is passed, send a data transfer request to the value data management platform, where the data transfer request includes the transfer-out value data and the value data management platform identity;

if value data of the innominate digital signature message for which transfer-out is to be done is greater than the transfer-out value data, determine a difference between the value data of the innominate digital signature message for which transfer-out is to be done and the transfer-out value data, as a second target difference;

update, according to the message identifier of the innominate digital signature message for which transfer-out is to be done and the message key of the innominate digital signature message for which transfer-out is to be done, the value data

of the innominate digital signature message for which transfer-out is to be done, to the second target difference; and

if the value data of the innominate digital signature message for which transfer-out is to be done is equal to the transfer-out value data, update, according to the message identifier of the innominate digital signature message for which transfer-out is to be done and the message key of the innominate digital signature message for which transfer-out is to be done, status of the innominate digital signature message for which transfer-out is to be done to be unavailable status.

[0394] Furthermore, the processing module 162 is further configured to:

determine whether or not the message identifier of the innominate digital signature message for which transfer-out is to be done matches the message key of the innominate digital signature message for which transfer-out is to be done; and determine, according to the message identifier of the innominate digital signature message for which transfer-out is to be done, whether or not the status of the innominate digital signature message for which transfer-out is to be done is available status, and whether or not the value data of the innominate digital signature message for which transfer-out is to be done is less than the transfer-out value data;

generate the sixth verification result that verification is passed, if the message identifier of the innominate digital signature message for which transfer-out is to be done matches the message key of the innominate digital signature message for which transfer-out is to be done and the status of the innominate digital signature message for which transfer-out is to be done is the available status and the value data of the innominate digital signature message for which transfer-out is to be done is greater than or equal to the transfer-out value data; and

generate the sixth verification result that verification is not passed, if the message identifier of the innominate digital signature message for which transfer-out is to be done does not match the message key of the innominate digital signature message for which transfer-out is to be done and/or the status of the innominate digital signature message for which transfer-out is to be done is the unavailable status and/or the value

data of the innominate digital signature message for which transfer-out is to be done is less than the transfer-out value data.

[0395] The data processing apparatus for the innominate digital signature message provided in the embodiment is configured to implement the technical solutions of the innominate digital signature message data management platform described in any of the aforementioned method embodiments, and implementation principles and technical effects thereof are similar and are not repeated here.

[0396] FIG. 17 is a schematic structural diagram of Embodiment 2 of a data processing apparatus for an innominate digital signature message provided by the present application. As shown in FIG. 17, a data processing apparatus 170 for the innominate digital signature message includes:

an obtaining module 171, configured to obtain, in response to a data transfer-in operation from a user, data transfer-in information input by the user, where the data transfer-in information includes a value data management platform identity, a value data management platform password, a transfer-in data flow direction identifier and transfer-in value data, and the transfer-in data flow direction identifier is an innominate digital signature message data management platform identity or a message identifier of an innominate digital signature message for which transfer-in is to be done;

a processing module 172, configured to transfer, according to the value data management platform identity and the value data management platform password and from an identity data set corresponding to the value data management platform identity, value data equal to the transfer-in value data into an innominate digital signature message general data set corresponding to an innominate digital signature message data management platform; and

a communicating module 173, configured to send a data transfer-in request to the innominate digital signature message data management platform, where the data transfer-in request includes the transfer-in data flow direction identifier and the transfer-in value data.

[0397] Furthermore, the obtaining module 171 is further configured to obtain, in

response to a data transfer-out operation from the user, transfer-out value data, the value data management platform identity, a message identifier of an innominate digital signature message for which transfer-out is to be done and a message key of the innominate digital signature message for which transfer-out is to be done input by the user; and

the communicating module 173 is further configured to send a data transfer-out request to the innominate digital signature message data management platform, where the data transfer-out request includes the transfer-out value data, the message identifier of the innominate digital signature message for which transfer-out is to be done and the message key of the innominate digital signature message for which transfer-out is to be done, and the value data management platform identity.

[0398] Furthermore, the communicating module 173 is further configured to receive a data transfer request sent by the innominate digital signature message data management platform, where the data transfer request includes transfer-out value data and the value data management platform identity; and

the processing module 172 is further configured to transfer, according to the value data management platform identity and from the innominate digital signature message general data set corresponding to the innominate digital signature message data management platform, value data equal to the transfer-out value data into the identity data set corresponding to the value data management platform identity.

[0399] The data processing apparatus for the innominate digital signature message provided in the embodiment is configured to implement the technical solutions of the value data management platform described in any of the aforementioned method embodiments, and implementation principles and technical effects thereof are similar and are not repeated here.

[0400] FIG. 18 is schematic structural diagram I of an electronic device provided by the present application. As shown in FIG. 18, an electronic device 180 includes:

a processor 181, a memory 182, and a communication interface 183;

the memory 182 is used to store an instruction executable by the processor

181; and

the processor 181 is configured to execute the technical solutions of the innominate digital signature message data management platform described in any of the aforementioned method embodiments by executing the instruction executable by the processor 181.

[0401] Optionally, the memory 182 may be independent or integrated with the processor 181.

[0402] Optionally, when the memory 182 is a component independent of the processor 181, the electronic device 180 may further include:

a bus 184, through which the memory 182 and the communication interface 183 are connected to the processor 181 and implement mutual communication, and the communication interface 183 is used for communicating with other devices.

[0403] Optionally, the communication interface 183 may specifically be implemented by a transceiver. The communication interface is used to realize the communication between a database access apparatus and other devices such as a client, a read-write library and a read-only library. The memory may include a random access memory (RAM), and may further include a non-volatile memory such as at least one disk memory.

[0404] The bus 184 may be a peripheral component interconnect (PCI) standard bus or an extended industry standard architecture (EISA) bus or the like. The bus can be divided into an address bus, a data bus, a control bus and so on. For ease of representation, only one thick line is used in the figure, but it does not mean that there is only one bus or one type of bus.

[0405] The above-mentioned processor can be a general-purpose processor, including a central processing unit (CPU), a network processor (NP) etc.; or can be a digital signal processor (DSP), an application-specific integrated circuit (ASIC), a field programmable gate array (FPGA) or other programmable logic components, a discrete gate or a transistor logic component, and a discrete hardware component.

[0406] The electronic device is configured to implement the technical solutions of

the innominate digital signature message data management platform described in any of the aforementioned method embodiments, and implementation principles and technical effects thereof are similar and are not repeated here.

[0407] FIG. 19 is schematic structural diagram II of an electronic device provided by the present application. As shown in FIG. 19, an electronic device 190 includes:

a processor 191, a memory 192, and a communication interface 193;
the memory 192 is used to store an instruction executable by the processor 191; and

the processor 191 is configured to execute the technical solutions of the value data management platform described in any of the aforementioned method embodiments by executing the instruction executable by the processor 191.

[0408] Optionally, the memory 192 may be independent or integrated with the processor 191.

[0409] Optionally, when the memory 192 is a component independent of the processor 191, the electronic device 190 may further include:

a bus 194, through which the memory 192 and the communication interface 193 are connected to the processor 191 and implement mutual communication, and the communication interface 193 is used for communicating with other devices.

[0410] Optionally, the communication interface 193 may specifically be implemented by a transceiver. The communication interface is used to realize the communication between a database access apparatus and other devices such as a client, a read-write library and a read-only library. The memory may include a random access memory (RAM), and may further include a non-volatile memory such as at least one disk memory.

[0411] The bus 194 may be a peripheral component interconnect (PCI) standard bus or an extended industry standard architecture (EISA) bus or the like. The bus can be divided into an address bus, a data bus, a control bus and so on. For ease of representation, only one thick line is used in the figure, but it does not mean that there is only one bus or one type of bus.

[0412] The above-mentioned processor can be a general-purpose processor, including a central processing unit (CPU), a network processor (NP) etc.; or can be a digital signal processor (DSP), an application-specific integrated circuit (ASIC), a field programmable gate array (FPGA) or other programmable logic components, a discrete gate or a transistor logic component, and a discrete hardware component.

[0413] The electronic device is configured to implement the technical solutions of the value data management platform described in any of the aforementioned method embodiments, and implementation principles and technical effects thereof are similar and are not repeated here.

[0414] An embodiment of the present application further provides a readable storage medium on which a computer program is stored, and when the computer program is executed by a processor, the technical solution provided by any one of the foregoing method embodiments is implemented.

[0415] An embodiment of the present application further provides a computer program product, including a computer program, and when the computer program is executed by a processor, the technical solution provided by any one of the foregoing method embodiments is implemented.

[0416] Those of ordinary skill in the art can understand that all or part of the steps for implementing the above method embodiments can be completed by program instructions and related hardware. The aforementioned program can be stored in a computer-readable storage medium. When the program is executed, the steps including the above-mentioned method embodiments are executed; and the aforementioned storage medium includes: a ROM, a RAM, a magnetic disk or an optical disk and other various media that can store program codes.

[0417] Finally, it should be noted that: the above embodiments are merely used for illustrating the technical solutions of the present application, rather than limiting them. Although the present application has been described in detail with reference to the foregoing embodiments, those skilled in the art should understand that they may still modify the technical solutions described in the foregoing embodiments, or make

equivalent substitutions for some or all of the technical features therein. These modifications or substitutions do not make the essence of the corresponding technical solutions deviate from the scope of the technical solutions of various embodiments of the present application.

CLAIMS

1. A data processing method for an innominate digital signature message, wherein the method is applied to an innominate digital signature message data management platform, and comprises:

5 receiving a data transfer-in request sent by a value data management platform, wherein the data transfer-in request comprises a transfer-in data flow direction identifier and transfer-in value data, and the transfer-in data flow direction identifier is an innominate digital signature message data management platform identity or a message identifier of an innominate digital signature message for which transfer-in is to be done;

10 generating a first target innominate digital signature message and determining a message identifier and a message key of the first target innominate digital signature message, if the transfer-in data flow direction identifier is the innominate digital signature message data management platform identity; and

15 determining the transfer-in value data as value data of the first target innominate digital signature message.

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

20 determining, according to the message identifier of the innominate digital signature message for which transfer-in is to be done, whether or not status of the innominate digital signature message for which transfer-in is to be done is available status, if the transfer-in data flow direction identifier is the message identifier of the innominate digital signature message for which transfer-in is to be done; and

25 updating, according to the transfer-in value data, value data of the innominate digital signature message for which transfer-in is to be done, if the status of the innominate digital signature message for which transfer-in is to be done is the available status.

3. The method according to claim 1, wherein if the transfer-in data flow direction identifier is the innominate digital signature message data management platform identity, the data transfer-in request further comprises signing-for duration information,

and the signing-for duration information is a signing-for duration or an unlimited signing-for duration identifier, and the method further comprises:

using the signing-for duration information as signing-for duration information of the first target innominate digital signature message;

- 5 if the signing-for duration information is the signing-for duration, generating a backflow innominate digital signature message and determining a message identifier and a message key of the backflow innominate digital signature message, wherein value data of the backflow innominate digital signature message is zero, and signing-for duration information of the backflow innominate digital signature message is the
- 10 unlimited signing-for duration identifier;

establishing and then storing a corresponding relationship between the message identifier of the backflow innominate digital signature message and the message identifier of the first target innominate digital signature message; and

- according to a current time and the signing-for duration information of the first
- 15 target innominate digital signature message, if monitoring that the first target innominate digital signature message has not been signed for within a time limit, updating status of the first target innominate digital signature message to be unavailable status, and updating, according to the corresponding relationship between the message identifier of the backflow innominate digital signature message and the message
- 20 identifier of the first target innominate digital signature message, the value data of the backflow innominate digital signature message to the value data of the first target innominate digital signature message.

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

- in response to an operation from a user for retrieving an innominate digital
- 25 signature message, obtaining a message identifier of a to-be-retrieved innominate digital signature message input by the user;

obtaining a retrieval result according to the message identifier of the to-be-retrieved innominate digital signature message, wherein the retrieval result comprises one or more of status of the to-be-retrieved innominate digital signature message, value

data of the to-be-retrieved innominate digital signature message, signing-for duration information of the to-be-retrieved innominate digital signature message, and a change record data set of the to-be-retrieved innominate digital signature message; and displaying the retrieval result.

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

in response to an operation from a user for signing for an innominate digital signature message to a new message, obtaining an innominate digital signature message data management platform identity of the user and, a message identifier of a to-be-signed-for innominate digital signature message and a message key of the to-be-signed-
10 for innominate digital signature message and signing-for duration information input by the user;

verifying, according to the message identifier of the to-be-signed-for innominate digital signature message and the message key of the to-be-signed-for innominate digital signature message, the to-be-signed-for innominate digital signature message to
15 generate a first verification result;

if the first verification result is that verification is passed, generating, according to the signing-for duration information input by the user, a second target innominate digital signature message, and determining a message identifier and a message key of the second target innominate digital signature message;

20 updating, according to the message identifier of the to-be-signed-for innominate digital signature message and the message key of the to-be-signed-for innominate digital signature message, status of the to-be-signed-for innominate digital signature message to be unavailable status; and

using value data of the to-be-signed-for innominate digital signature message as
25 value data of the second target innominate digital signature message.

6. The method according to claim 5, wherein the verifying, according to the message identifier of the to-be-signed-for innominate digital signature message and the message key of the to-be-signed-for innominate digital signature message, the to-be-signed-for innominate digital signature message to generate the first verification result

comprises:

determining whether or not the message identifier of the to-be-signed-for innominate digital signature message matches the message key of the to-be-signed-for innominate digital signature message; and determining, according to the message
5 identifier of the to-be-signed-for innominate digital signature message, whether or not the status of the to-be-signed-for innominate digital signature message is available status, and whether or not the value data of the to-be-signed-for innominate digital signature message is zero;

generating the first verification result that verification is passed, if the message
10 identifier of the to-be-signed-for innominate digital signature message matches the message key of the to-be-signed-for innominate digital signature message and the status of the to-be-signed-for innominate digital signature message is the available status and the value data of the to-be-signed-for innominate digital signature message is not zero;
and

15 generating the first verification result that verification is not passed, if the message identifier of the to-be-signed-for innominate digital signature message does not match the message key of the to-be-signed-for innominate digital signature message and/or the status of the to-be-signed-for innominate digital signature message is unavailable status and/or the value data of the to-be-signed-for innominate digital signature message
20 is zero.

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

in response to an operation from a user for signing for an innominate digital signature message to an existing message, obtaining a message identifier of a to-be-signed-for innominate digital signature message and a message key of the to-be-signed-
25 for innominate digital signature message and a message identifier of an innominate digital signature message for which transfer-in is to be done input by the user;

verifying, according to the message identifier of the to-be-signed-for innominate digital signature message, the message key of the to-be-signed-for innominate digital signature message and the message identifier of the innominate digital signature

message for which transfer-in is to be done, both the to-be-signed-for innominate digital signature message and the innominate digital signature message for which transfer-in is to be done, to generate a second verification result;

5 if the second verification result is that verification is passed, updating, according to value data of the to-be-signed-for innominate digital signature message, value data of the innominate digital signature message for which transfer-in is to be done; and

updating, according to the message identifier of the to-be-signed-for innominate digital signature message and the message key of the to-be-signed-for innominate digital signature message, status of the to-be-signed-for innominate digital signature
10 message to be unavailable status.

8. The method according to claim 7, wherein the verifying, according to the message identifier of the to-be-signed-for innominate digital signature message, the message key of the to-be-signed-for innominate digital signature message and the message identifier of the innominate digital signature message for which transfer-in is
15 to be done, both the to-be-signed-for innominate digital signature message and the innominate digital signature message for which transfer-in is to be done, to generate the second verification result comprises:

determining whether or not the message identifier of the to-be-signed-for innominate digital signature message matches the message key of the to-be-signed-for
20 innominate digital signature message; and determining, according to the message identifier of the to-be-signed-for innominate digital signature message and the message identifier of the innominate digital signature message for which transfer-in is to be done, whether or not the status of the to-be-signed-for innominate digital signature message is available status, whether or not the value data of the to-be-signed-for innominate
25 digital signature message is zero, and whether or not status of the innominate digital signature message for which transfer-in is to be done is available status;

generating the second verification result that verification is passed, if the message identifier of the to-be-signed-for innominate digital signature message matches the message key of the to-be-signed-for innominate digital signature message and the status

of the to-be-signed-for innominate digital signature message is the available status and the value data of the to-be-signed-for innominate digital signature message is not zero and the status of the innominate digital signature message for which transfer-in is to be done is the available status; and

- 5 generating the second verification result that verification is not passed, if the message identifier of the to-be-signed-for innominate digital signature message does not match the message key of the to-be-signed-for innominate digital signature message and/or the status of the to-be-signed-for innominate digital signature message is unavailable status and/or the value data of the to-be-signed-for innominate digital signature message is zero and/or the status of the innominate digital signature message
10 for which transfer-in is to be done is unavailable status.

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

- in response to an operation from a user for splitting an innominate digital signature message, obtaining an innominate digital signature message data management platform
15 identity of the user and, a message identifier of a to-be-split innominate digital signature message and a message key of the to-be-split innominate digital signature message, a total number of split innominate digital signature messages, and value data of each of the split innominate digital signature messages and signing-for duration information of each of the split innominate digital signature messages input by the user;

- 20 verifying, according to the message identifier of the to-be-split innominate digital signature message and the message key of the to-be-split innominate digital signature message and the value data of each of the split innominate digital signature messages, the to-be-split innominate digital signature message to generate a third verification result;

- 25 if the third verification result is that verification is passed, generating, according to the total number of the split innominate digital signature messages and the value data and the signing-for duration information of each of the split innominate digital signature messages, the split innominate digital signature messages, and determining a message identifier and a message key of each of the split innominate digital signature messages;

if a sum of value data of all the split innominate digital signature messages is equal to value data of the to-be-split innominate digital signature message, updating, according to the message identifier of the to-be-split innominate digital signature message and the message key of the to-be-split innominate digital signature message,
5 status of the to-be-split innominate digital signature message to be unavailable status;

if the sum of the value data of all the split innominate digital signature messages is less than the value data of the to-be-split innominate digital signature message, determining a difference between the value data of the to-be-split innominate digital signature message and the sum of the value data of all the split innominate digital
10 signature messages, as a first target difference; and

updating, according to the message identifier of the to-be-split innominate digital signature message and the message key of the to-be-split innominate digital signature message, the value data of the to-be-split innominate digital signature message to the first target difference.

15 10. The method according to claim 9, wherein the verifying, according to the message identifier of the to-be-split innominate digital signature message and the message key of the to-be-split innominate digital signature message and the value data of each of the split innominate digital signature messages, the to-be-split innominate digital signature message to generate the third verification result comprises:

20 determining whether or not the message identifier of the to-be-split innominate digital signature message matches the message key of the to-be-split innominate digital signature message; and determining, according to the message identifier of the to-be-split innominate digital signature message and the value data of each of the split innominate digital signature messages, whether or not the status of the to-be-split
25 innominate digital signature message is available status, whether or not the value data of the to-be-split innominate digital signature message is zero, and whether or not the sum of the value data of all the split innominate digital signature messages is greater than the value data of the to-be-split innominate digital signature message;

generating the third verification result that verification is passed, if the message

identifier of the to-be-split innominate digital signature message matches the message key of the to-be-split innominate digital signature message and the status of the to-be-split innominate digital signature message is the available status and the value data of the to-be-split innominate digital signature message is not zero and the sum of the value data of all the split innominate digital signature messages is less than or equal to the value data of the to-be-split innominate digital signature message; and

generating the third verification result that verification is not passed, if the message identifier of the to-be-split innominate digital signature message does not match the message key of the to-be-split innominate digital signature message and/or the status of the to-be-split innominate digital signature message is the unavailable status and/or the value data of the to-be-split innominate digital signature message is zero and/or the sum of the value data of all the split innominate digital signature messages is greater than the value data of the to-be-split innominate digital signature message.

11. The method according to claim 9, further comprising:

for each of the split innominate digital signature messages,
if signing-for duration information of a split innominate digital signature message is a signing-for duration, generating a backflow innominate digital signature message and determining a message identifier and a message key of the backflow innominate digital signature message, wherein value data of the backflow innominate digital signature message is zero, and signing-for duration information of the backflow innominate digital signature message is an unlimited signing-for duration identifier;

establishing and then storing a corresponding relationship between the message identifier of the backflow innominate digital signature message and the message identifier of the split innominate digital signature message; and

according to a current time and the signing-for duration information of the split innominate digital signature message, if monitoring that the split innominate digital signature message has not been signed for within a time limit, updating status of the split innominate digital signature message to be unavailable status, and updating, according to the corresponding relationship between the message identifier of the

backflow innominate digital signature message and the message identifier of the split innominate digital signature message, the value data of the backflow innominate digital signature message to value data of the split innominate digital signature message.

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

5 in response to an operation from a user for merging innominate digital signature messages into a new message, obtaining an innominate digital signature message data management platform identity of the user and, message identifiers of a plurality of to-be-merged innominate digital signature messages and message keys of the plurality of to-be-merged innominate digital signature messages and signing-for duration
10 information input by the user;

verifying, according to the message identifiers of the plurality of to-be-merged innominate digital signature messages and the message keys of the plurality of to-be-merged innominate digital signature messages, the plurality of to-be-merged innominate digital signature messages to generate a fourth verification result;

15 if the fourth verification result is that verification is passed, generating, according to the signing-for duration information input by the user, a third target innominate digital signature message, and determining a message identifier and a message key of the third target innominate digital signature message;

20 updating, according to the message identifiers of the plurality of to-be-merged innominate digital signature messages and the message keys of the plurality of to-be-merged innominate digital signature messages, status of the plurality of to-be-merged innominate digital signature messages to be unavailable status; and

25 using a sum of value data of the plurality of to-be-merged innominate digital signature messages as value data of the third target innominate digital signature message.

13. The method according to claim 12, wherein the verifying, according to the message identifiers of the plurality of to-be-merged innominate digital signature messages and the message keys of the plurality of to-be-merged innominate digital signature messages, the plurality of to-be-merged innominate digital signature

messages to generate the fourth verification result comprises:

determining whether or not a message identifier of each to-be-merged innominate digital signature message matches a message key of each to-be-merged innominate digital signature message; and determining, according to the message identifiers of the plurality of to-be-merged innominate digital signature messages, whether or not the status of all the to-be-merged innominate digital signature messages is available status;

generating the fourth verification result that verification is passed, if the message identifier of each to-be-merged innominate digital signature message matches the message key of each to-be-merged innominate digital signature message and the status of all the to-be-merged innominate digital signature messages is the available status; and

generating the fourth verification result that verification is not passed, if there is at least one to-be-merged innominate digital signature message whose message identifier and message key do not match each other and/or there is at least one to-be-merged innominate digital signature message whose status is the unavailable status.

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

if the signing-for duration information is a signing-for duration, generating a backflow innominate digital signature message and determining a message identifier and a message key of the backflow innominate digital signature message, wherein value data of the backflow innominate digital signature message is zero, and signing-for duration information of the backflow innominate digital signature message is an unlimited signing-for duration identifier;

establishing and then storing a corresponding relationship between the message identifier of the backflow innominate digital signature message and the message identifier of the third target innominate digital signature message; and

according to a current time and signing-for duration information of the third target innominate digital signature message, if monitoring that the third target innominate digital signature message has not been signed for within a time limit, updating status of the third target innominate digital signature message to be unavailable status, and

updating, according to the corresponding relationship between the message identifier of the backflow innominate digital signature message and the message identifier of the third target innominate digital signature message, the value data of the backflow innominate digital signature message to the value data of the third target innominate digital signature message.

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

in response to an operation from a user for merging an innominate digital signature message into an existing message, obtaining a message identifier of a fourth target innominate digital signature message and a message key of the fourth target innominate digital signature message and a message identifier of at least one to-be-merged innominate digital signature message and a message key of the at least one to-be-merged innominate digital signature message input by the user;

verifying, according to the message identifier of the fourth target innominate digital signature message and the message key of the fourth target innominate digital signature message and the message identifier of the at least one to-be-merged innominate digital signature message and the message key of the at least one to-be-merged innominate digital signature message, both the fourth target innominate digital signature message and the at least one to-be-merged innominate digital signature message to generate a fifth verification result;

if the fifth verification result is that verification is passed, updating, according to value data of the at least one to-be-merged innominate digital signature message, value data of the fourth target innominate digital signature message; and

updating, according to the message identifier of the at least one to-be-merged innominate digital signature message and the message key of the at least one to-be-merged innominate digital signature message, status of the at least one to-be-merged innominate digital signature message to be unavailable status.

16. The method according to claim 15, wherein the verifying, according to the message identifier of the fourth target innominate digital signature message and the message key of the fourth target innominate digital signature message and the message

identifier of the at least one to-be-merged innominate digital signature message and the message key of the at least one to-be-merged innominate digital signature message, both the fourth target innominate digital signature message and the at least one to-be-merged innominate digital signature message to generate the fifth verification result
5 comprises:

determining whether or not the message identifier of the fourth target innominate digital signature message matches the message key of the fourth target innominate digital signature message and whether or not the message identifier of each to-be-merged innominate digital signature message matches the message key of the each to-
10 be-merged innominate digital signature message; and determining, according to the message identifier of the fourth target innominate digital signature message and the message identifier of the at least one to-be-merged innominate digital signature message, whether or not status of the fourth target innominate digital signature message is available status and whether or not status of all of the at least one to-be-merged
15 innominate digital signature message is available status;

generating the fifth verification result that verification is passed, if the message identifier of the fourth target innominate digital signature message matches the message key of the fourth target innominate digital signature message and the message identifier of each to-be-merged innominate digital signature message matches the message key
20 of the each to-be-merged innominate digital signature message and the status of the fourth target innominate digital signature message is the available status and the status of all of the at least one to-be-merged innominate digital signature message is the available status; and

generating the fifth verification result that verification is not passed, if the message
25 identifier of the fourth target innominate digital signature message does not match the message key of the fourth target innominate digital signature message and/or there is at least one to-be-merged innominate digital signature message whose message identifier and message key do not match each other and/or the status of the fourth target innominate digital signature message is unavailable status and/or there is at least one

to-be-merged innominate digital signature message whose status is unavailable status.

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

obtaining a data transfer-out request, wherein the data transfer-out request comprises transfer-out value data, a message identifier of an innominate digital signature message for which transfer-out is to be done and a message key of the to-be-transferred-out innominate digital signature message, and a value data management platform identity, and the data transfer-out request is sent by the value data management platform, or, the data transfer-out request is generated, in response to a data transfer-out operation from a user, according to the transfer-out value data, the value data management platform identity, the message identifier of the innominate digital signature message for which transfer-out is to be done and the message key of the innominate digital signature message for which transfer-out is to be done input by the user;

verifying, according to the message identifier of the innominate digital signature message for which transfer-out is to be done and the message key of the innominate digital signature message for which transfer-out is to be done, the innominate digital signature message for which transfer-out is to be done to generate a sixth verification result;

if the sixth verification result is that verification is passed, sending a data transfer request to the value data management platform, wherein the data transfer request comprises the transfer-out value data and the value data management platform identity;

if value data of the innominate digital signature message for which transfer-out is to be done is greater than the transfer-out value data, determining a difference between the value data of the innominate digital signature message for which transfer-out is to be done and the transfer-out value data, as a second target difference;

updating, according to the message identifier of the innominate digital signature message for which transfer-out is to be done and the message key of the innominate digital signature message for which transfer-out is to be done, the value data of the innominate digital signature message for which transfer-out is to be done to the second

target difference; and

if the value data of the innominate digital signature message for which transfer-out is to be done is equal to the transfer-out value data, updating, according to the message identifier of the innominate digital signature message for which transfer-out is to be done and the message key of the innominate digital signature message for which transfer-out is to be done, status of the innominate digital signature message for which transfer-out is to be done to be unavailable status.

18. The method according to claim 17, wherein the verifying, according to the message identifier of the innominate digital signature message for which transfer-out is to be done and the message key of the innominate digital signature message for which transfer-out is to be done, the innominate digital signature message for which transfer-out is to be done to generate the sixth verification result comprises:

determining whether or not the message identifier of the innominate digital signature message for which transfer-out is to be done matches the message key of the innominate digital signature message for which transfer-out is to be done; and determining, according to the message identifier of the innominate digital signature message for which transfer-out is to be done, whether or not the status of the innominate digital signature message for which transfer-out is to be done is available status, and whether or not the value data of the innominate digital signature message for which transfer-out is to be done is less than the transfer-out value data;

generating the sixth verification result that verification is passed, if the message identifier of the innominate digital signature message for which transfer-out is to be done matches the message key of the innominate digital signature message for which transfer-out is to be done and the status of the innominate digital signature message for which transfer-out is to be done is the available status and the value data of the innominate digital signature message for which transfer-out is to be done is greater than or equal to the transfer-out value data; and

generating the sixth verification result that verification is not passed, if the message identifier of the innominate digital signature message for which transfer-out is

to be done does not match the message key of the innominate digital signature message for which transfer-out is to be done and/or the status of the innominate digital signature message for which transfer-out is to be done is the unavailable status and/or the value data of the innominate digital signature message for which transfer-out is to be done is less than the transfer-out value data.

19. A data processing method for an innominate digital signature message, wherein the method is applied to a value data management platform and comprises:

in response to a data transfer-in operation from a user, obtaining data transfer-in information input by the user, wherein the data transfer-in information comprises a value data management platform identity, a value data management platform password, a transfer-in data flow direction identifier and transfer-in value data, and the transfer-in data flow direction identifier is an innominate digital signature message data management platform identity or a message identifier of an innominate digital signature message for which transfer-in is to be done;

transferring, according to the value data management platform identity and the value data management platform password and from an identity data set corresponding to the value data management platform identity, value data equal to the transfer-in value data into an innominate digital signature message general data set corresponding to an innominate digital signature message data management platform; and

sending a data transfer-in request to the innominate digital signature message data management platform, wherein the data transfer-in request comprises the transfer-in data flow direction identifier and the transfer-in value data.

20. The method according to claim 19, further comprising:

in response to a data transfer-out operation from the user, obtaining transfer-out value data, the value data management platform identity, a message identifier of an innominate digital signature message for which transfer-out is to be done and a message key of the innominate digital signature message for which transfer-out is to be done input by the user; and

sending a data transfer-out request to the innominate digital signature message data

management platform, wherein the data transfer-out request comprises the transfer-out value data, the message identifier of the innominate digital signature message for which transfer-out is to be done and the message key of the innominate digital signature message for which transfer-out is to be done, and the value data management platform
5 identity.

21. The method according to claim 19, further comprising:

receiving a data transfer request sent by the innominate digital signature message data management platform, wherein the data transfer request comprises transfer-out value data and the value data management platform identity; and

10 transferring, according to the value data management platform identity and from the innominate digital signature message general data set corresponding to the innominate digital signature message data management platform, value data equal to the transfer-out value data into the identity data set corresponding to the value data management platform identity.

15 22. A data processing apparatus for an innominate digital signature message, comprising:

a communicating module, configured to receive a data transfer-in request sent by a value data management platform, wherein the data transfer-in request comprises a transfer-in data flow direction identifier and transfer-in value data, and the transfer-in
20 data flow direction identifier is an innominate digital signature message data management platform identity or a message identifier of an innominate digital signature message for which transfer-in is to be done; and

a processing module, configured to:

generate a first target innominate digital signature message and determine a
25 message identifier and a message key of the first target innominate digital signature message, if the transfer-in data flow direction identifier is the innominate digital signature message data management platform identity; and

determine the transfer-in value data as value data of the first target innominate digital signature message.

23. A data processing apparatus for an innominate digital signature message, comprising:

an obtaining module, configured to obtain, in response to a data transfer-in operation from a user, data transfer-in information input by the user, wherein the data transfer-in information comprises a value data management platform identity, a value data management platform password, a transfer-in data flow direction identifier and transfer-in value data, and the transfer-in data flow direction identifier is an innominate digital signature message data management platform identity or a message identifier of an innominate digital signature message for which transfer-in is to be done;

10 a processing module, configured to transfer, according to the value data management platform identity and the value data management platform password and from an identity data set corresponding to the value data management platform identity, value data equal to the transfer-in value data into an innominate digital signature message general data set corresponding to an innominate digital signature message data management platform; and

15 a communicating module, configured to send a data transfer-in request to the innominate digital signature message data management platform, wherein the data transfer-in request comprises the transfer-in data flow direction identifier and the transfer-in value data.

20 24. An electronic device, comprising:

a processor, a memory, and a communication interface;

wherein the memory is used to store an instruction which is executable by the processor; and

25 the processor is configured to execute the data processing method for the innominate digital signature message according to any one of claims 1 to 18 by executing the instruction which is executable by the processor.

25. An electronic device, comprising:

a processor, a memory, and a communication interface;

wherein the memory is used to store an instruction which is executable by the

processor; and

the processor is configured to execute the data processing method for the innominate digital signature message according to any one of claims 19 to 21 by executing the instruction which is executable by the processor.

5 26. A readable storage medium storing a computer program, wherein when the computer program is executed by a processor, the data processing method for the innominate digital signature message according to any one of claims 1 to 21 is implemented.

10 27. A computer program product, comprising a computer program, wherein when the computer program is executed by a processor, the data processing method for the innominate digital signature message according to any one of claims 1 to 21 is implemented.