Innovation, Sciences et Développement économique Canada
Office de la Propriété Intellectuelle du Canada

Innovation, Science and Economic Development Canada
Canadian Intellectual Property Office

CA 3123658 C 2023/01/10

(11)(21) 3 123 658

(12) BREVET CANADIEN
CANADIAN PATENT

(13) C

(22) Date de dépôt/Filing Date: 2015/07/21

(41) Mise à la disp. pub./Open to Public Insp.: 2017/01/26

(45) Date de délivrance/Issue Date: 2023/01/10

(62) Demande originale/Original Application: 2 993 090

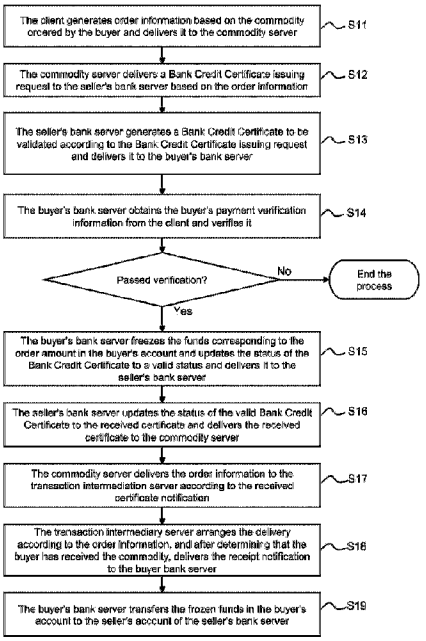
(51) Cl.Int./Int.Cl. *G06Q 20/40* (2012.01), *H04L 9/06* (2006.01), *H04L 9/08* (2006.01)

(72) Inventeur/Inventor:
ZHANG, YI, CN

(73) Propriétaire/Owner:
10353744 CANADA LTD., CA

(74) Agent: HINTON, JAMES W.

(54) Titre : PROCEDE, DISPOSITIF ET SYSTEME DE TRANSACTION EN LIGNE
(54) Title: ONLINE TRANSACTION METHOD, DEVICE AND SYSTEM



(57) Abrégé/Abstract:
Disclosed are an online transaction method, device and system, the method comprising the steps of: an item server sends a bank credit certificate issuing request to a seller bank server according to order information; the seller bank server generates a bank credit certificate having a to-be-effective status, and sends the bank credit certificate to a buyer bank server; the buyer bank server verifies buyer payment checking information obtained by a client, and after verification has been passed, freezes funds in a buyer account which correspond to an order amount, updates the status of the bank credit certificate to an effective status, and sends the bank credit certificate to the seller bank server; the seller bank server sends a has-been-received notification to the item server; the item server sends the order information to a transaction intermediary server; the transaction intermediary server dispatches according to arrangements, and sends a has-been-received notification to the buyer bank server; the buyer bank server transfers the frozen funds in the buyer account into a seller account of the seller bank server. The present invention reduces the risk to the funds, and increases the security of the transaction information.

Abstract

Disclosed are an online transaction method, device and system, the method comprising the steps of: an item server sends a bank credit certificate issuing request to a seller bank server according to order information; the seller bank server generates a bank credit certificate having a to-be-effective status, and sends the bank credit certificate to a buyer bank server; the buyer bank server verifies buyer payment checking information obtained by a client, and after verification has been passed, freezes funds in a buyer account which correspond to an order amount, updates the status of the bank credit certificate to an effective status, and sends the bank credit certificate to the seller bank server; the seller bank server sends a has-been-received notification to the item server; the item server sends the order information to a transaction intermediary server; the transaction intermediary server dispatches according to arrangements, and sends a has-been-received notification to the buyer bank server; the buyer bank server transfers the frozen funds in the buyer account into a seller account of the seller bank server. The present invention reduces the risk to the funds, and increases the security of the transaction information.

Date Reçue/Date Received 2021-04-20

Online Transaction Method, Device And System

Technical Field

[0001] The present invention relates to the field of Internet technology, and in particular, to an online transaction method, device, and system.

Background Technology

[0002] With the rapid development of Internet technology, E-commerce has been booming around the world, with online trading platforms such as Amazon, Alibaba, Taobao and other E-commerce as the main mode of operation of the online trading platform. At present, transaction payments on online trading platforms can usually be paid on the Internet, on delivery and mail order and other means. Due to the long transaction time and high transaction cost, traditional payment methods such as cash on delivery and mail order cannot meet the growing E-commerce behaviour and also have high security problems. Therefore, these payment methods are rarely used, and online banking is increasingly becoming the mainstream of payment.

[0003] In the existing technology, online payment methods mainly use third-party payment platform. During the transaction, the buyer transfers the transaction funds to the third-party payment platform, and the third-party payment platform stores the transaction information at the same time. After the buyer receives the commodity, the third-party payment platform transfers the transaction funds to the seller, and the transaction is completed.

[0004] However, this method, which is temporarily deposited by third-party payment platforms and trading information, often occurs in the following situations: when the customer has not yet received the commodity or services provided by the merchant and the funds have been paid by the third-party payment institution to the merchant; Or merchants provided the commodity or services, the customer has been unable to pay the corresponding funds. It can be seen that, due to the outflow of trading funds out of the banking system, the payment of bank servers is completely dependent on the operation of third-party payment platforms, which is not conducive to the supervision of funds by banks. When the above situation occurs in the third-party payment platform, the bank server is not able to make the effective capital flow of the delivery of the first hand, which may result in large deviation of the cash flow time of the bank server from the actual transaction time to the user it may bring financial risk to users, and trading funds and transaction information in the third-party payment platform information has the risk of being stolen, the security is not high. Thus it can be seen that at this stage an improved transaction method is needed to reduce the risk of capital and improve the security

Date Reçue/Date Received 2021-04-20

of transaction information.

Technical problem

[0005] The main object of the present invention is to provide a method, device and system for online transactions aimed at reducing capital risk and improve transaction security.

Problem solving solution

Technical solutions

[0006] The technical solution of the present invention to solve the above-mentioned technical problems is as follows:

[0007] According to one aspect of the present invention, there is provided an online transaction method including the steps of:

[0008] After receiving the order information delivered by the client, the commodity server delivers a Bank Credit Certificate issuing request to the seller's bank server according to the order information;

[0009] The seller's bank server generates a Bank Credit Certificate to be validated according to the Bank Credit Certificate issuing request, and delivers the Bank Credit Certificate to the buyer's bank server;

[0010] The buyer bank server obtains the buyer's payment verification information from the client and performs verification; when the verification passes, the buyer bank account funds corresponding to the order amount are frozen, and the state of the Bank Credit Certificate is updated to the valid status and delivered to the seller's bank server;

[0011] The seller's bank server updates the status of the validated Bank Credit Certificate to a received certificate and delivers a received card notification to the commodity server;

[0012] The commodity server delivers the order information to the transaction intermediation server according to the received card notification;

[0013] The transaction intermediary server arranges the commodity according to the order information and delivers a receipt notification to the buyer's bank server after determining that the buyer has received the commodity;

[0014] After receiving the commodity receipt notification, the buyer bank server transfers the funds frozen in the buyer's account to the seller's account of the seller's bank server.

[0015] According to another aspect of the present invention, it is provided an online transaction method applied to a commodity server, the method including the steps of:

[0016] After receiving the order information delivered by the client, delivers a Bank Credit Certificate

Date Reçue/Date Received 2021-04-20

issuing request to the seller's bank server according to the order information;

[0017] After receiving the received card notification delivered by the seller's bank server, the order information is delivered to a transaction intermediation server.

[0018] According to another aspect of the present invention, it is provided an online transaction method applied to a seller's bank server, the method including the steps of:

[0019] After receiving the Bank Credit Certificate issuing request delivered by the commodity server, a Bank Credit Certificate to be validated is generated and delivered to the buyer's bank server;

[0020] After receiving the effective Bank Credit Certificate delivered by the buyer's Bank server, the status of the Bank Credit Certificate is updated to the accepted status, and the received notification is delivered to the commodity server.

[0021] According to another aspect of the present invention, it is provided an online transaction method applied to a buyer's bank server, the method including the steps of:

[0022] After receiving the Bank Credit Certificate to be effective, the buyer's payment verification information is acquired from the client and verified;

[0023] if the verification is passed, the funds in the buyer account corresponding to the order amount are frozen, and the status of the Bank Credit Certificate is updated to the effective and delivered to the seller bank server;

[0024] After receiving the received notification delivered by the transaction intermediation server, the funds frozen in the buyer's account are transferred to the seller's account of the seller's bank server.

[0025] According to another aspect of the present invention, it is provided an online transaction system including a client used to generate order information based on items ordered by a buyer, a commodity server, a buyer's bank server, a seller's bank server, and a transaction intermediation server, wherein:

[0026] The commodity server is used to deliver a request for issuing a Bank Credit Certificate to the seller's bank server after receiving the order information delivered by the client; after receiving the received certificate delivered by the seller's bank server, deliver the order information to the transaction intermediation server after the notification;

[0027] The seller's bank server is used to generate a Bank Credit Certificate of a to-be-validated state after receiving the Bank Credit Certificate issuing request and deliver the Bank Credit Certificate to the buyer's bank server; and after receiving the Bank Credit Certificate delivered by the buyer's bank server after the valid Bank Credit Certificate is updated, the status of the

Date Reçue/Date Received 2021-04-20

Bank Credit Certificate is updated to the certified status and the received credit notification is delivered to the commodity server;

[0028] The transaction intermediary server is set to arrange delivery according to the order information and deliver a receipt notification to the buyer's bank server after determining that the buyer has received the commodity;

[0029] The buyer bank server is set to receive the Bank Credit Certificate to be validated, acquires the buyer's payment verification information from the client and performs verification; when the verification is passed, the buyer's account is frozen, and update the status of the Bank Credit Certificate to a valid status and deliver the status to the seller's bank server; and after receiving the received notification, transfer the funds frozen in the buyer's account to the seller's bank account in the seller's server.

[0030] According to another aspect of the present invention, it is provided an online transaction device applied to a commodity server, including the following modules:

[0031] The first receiving module is used to receive the order information delivered by the client and the received card notification delivered by the seller's bank server;

[0032] The issuing request module is used to deliver a Bank Credit Certificate issuing request to the seller bank server according to the order information after receiving the order information delivered by the client;

[0033] The order information delivery module is used to deliver the order information to the transaction intermediation server after receiving the received card notification delivered by the seller's bank server.

[0034] According to another aspect of the present invention, it is provided an online transaction device applied to a seller's bank server, the device includes the following modules:

[0035] A second receiving module is used to receive a Bank Credit Certificate issuing request delivered by the commodity server and an effective Bank Credit Certificate delivered by the buyer's bank server;

[0036] A Bank Credit Certificate generating module is used to generate a Bank Credit Certificate which is in effect according to a Bank Credit Certificate issuing request;

[0037] A Bank Credit Certificate delivery module is used to deliver the Bank Credit Certificate to be validated to the buyer bank server;

[0038] The received module notification module is used to receive the Bank Credit Certificate valid from the buyer bank server, update the status of the Bank Credit Certificate to the certified

Date Reçue/Date Received 2021-04-20

status, and deliver the received certificate to the commodity server.

[0039] According to another aspect of the present invention, it is provided an online transaction device applied to a buyer's bank server, the device includes the following modules:

[0040] A third receiving module is used to receive a Bank Credit Certificate delivered by the seller's bank server and to be validated and a receipt notification delivered by the transaction intermediation server;

[0041] The verification module is used to receive the buyer's payment verification information from the client and verify it after receiving the Bank Credit Certificate of the to-be-validated state;

[0042] A freezing module is used to freeze the funds corresponding to the order amount in the buyer's account after verification is passed and update the status of the Bank Credit Certificate to be valid and deliver the status to the seller's bank server;

[0043] A money transfer module is used to, after receiving the commodity receipt notification, the buyer bank server transfers the funds frozen in the buyer's account to the seller's account of the seller's bank server.

[0044] The online trading method, device and system provided by the present invention, deliver the issuing request to the seller's bank server through the commodity server, the intermediary transaction server delivers the receiving notification to the buyer's bank server, the client, the commodity server, the buyer's bank server, the seller's bank server and the transaction intermediary server to complete the transaction process, the transaction process of transaction funds, transaction information does not go to the third-party payment platform, and all flow within the banking system, thus , it is convenient for the bank to supervise the funds, improve the security of the transaction, and also facilitate the supervision of the credit of the subject of the transaction, which is conducive to the establishment of the social credit system. And the transaction status is monitored in real time by generating Bank Credit Certificate so that there is no deviation between the time of fund flow and the actual transaction time, so that it can effectively reduce the risk of funds and improve the security of the transaction information.

The beneficial effect of the invention

Beneficial effect

[0045] Further, in the transaction process, it also use of digital envelope technology to secure the transmission of communications data, the use of dynamic anti-counterfeiting technology to dynamically generate a symmetric key, the use of AES encryption algorithm to encrypt data, the use of double-track calibration technology to verify the data, using two networks and use

Date Reçue/Date Received 2021-04-20

technology to communicate, to further improve the security of the transaction.

A brief description of the drawings

Brief Description

[0046] Figure 1 is a flowchart of a first example of the online transaction method of the present invention;

[0047] Figure 2 is an interactive diagram of each system in a transaction process in an example of the present invention;

[0048] Figure 3 is a specific flow chart of the data deliverer and the data receiver adopting the digital envelope technology to securely transmit the communication data in the example of the present invention;

[0049] Figure 4 is a flowchart of a second example of the online transaction method of the present invention;

[0050] Figure 5 is a flowchart of the third example of the online transaction method of the present invention;

[0051] Figure 6 is a flowchart of a fourth example of the online transaction method of the present invention;

[0052] Figure 7 is a flow chart of the fifth example of the online transaction method of the present invention;

[0053] Figure 8 is a block diagram of the first example of the online trading system of the present invention;

[0054] Figure 9 is a schematic block diagram of an example of an online transaction device applied to a client according to the present invention;

[0055] Figure 10 is a block schematic diagram of an example of an online trading device applied to a commodity server according to the present invention;

[0056] Figure 11 is a schematic block diagram of an example of an online transaction device applied to a seller's bank server according to the present invention;

[0057] Figure 12 is a schematic block diagram of an example of an online transaction device applied to a buyer's bank server according to the present invention;

[0058] Figure 13 is a schematic block diagram of an example of an online transaction device applied to a transaction intermediation server according to the present invention;

[0059] Figure 14 is a schematic block diagram of a second example of the online trading system of the present invention.

Date Reçue/Date Received 2021-04-20

[0060] The realization of the object of the present invention, features and advantages of the present invention will be further described with reference to the accompanying drawings.

Examples of the Invention

Implementation pattern of the present invention

[0061] It is to be understood that the specific examples described herein are merely illustrative of the invention but not intended to limit the invention.

[0062] Please refer to Figure 1 and Figure 2, an example of the online transaction method of the present invention is proposed, and the method includes the following steps:

[0063] S11: the client generates order information according to the commodity information ordered by the buyer and delivers it to the commodity server.

[0064] In step S11, the seller inputs and stores the commodity information into the commodity server, and the buyer communicates with the commodity server through the client to obtain the commodity information from the commodity server. The buyer selects the commodity to be purchased in the commodity information, the client generates the order information according to the commodity information selected by the user, and submits the order information to the commodity server.

[0065] In this example, the commodity includes tangible physical commodity and invisible services; the commodity information includes information such as commodity prices and parameters; the commodity server may be a commercial computer server or a seller's own computer server; the client is a communication terminal operated by the buyer, and may be a terminal device such as a mobile phone, a tablet, a computer or the terminal device.

[0066] S12: the commodity server delivers a Bank Credit Certificate issuing request to the seller's bank server according to the order information.

[0067] In this example, the buyer's bank server refers to the computer server of the buyer's bank account (i.e., the buyer's bank), and the seller's bank server refers to the seller's bank account corresponding to the bank (i.e., the seller's account bank), the buyer's bank server and the seller's bank server may be the same bank's computer server (i.e., the buyer's and seller's bank of accounts are the same) or the computers of different banks (i.e., the buyer's and seller's bank are not at the same time).

[0068] In step S12, after receiving the order information, the commodity server learns the buyer bank server and the seller bank server according to the order information, generates a bank credit certificate issuing request, and delivers the request to the seller bank server. Wherein, Bank

Date Reçue/Date Received 2021-04-20

Credit Certificate is an electronic certificate committed by a bank, which can be interpreted as an electronic data that can be stored in a computer system and transmitted over the Internet.

[0069] S13: the seller's bank server generates a Bank Credit Certificate to be validated according to the Bank Credit Certificate issuing request, and delivers it to the buyer's bank server.

[0070] In this step S13, after receiving the issuing request of Bank Credit Certificate, the seller's bank server learns the buyer's bank server and generates a Bank Credit Certificate Z1 to be validated and delivers it to the buyer's bank server.

[0071] S14: the buyer bank server obtains the buyer's payment verification information from the client and performs verification. If the verification is passed, step S15 is performed; otherwise, the process ends.

[0072] In this step S14, after receiving the Bank Credit Certificate Z1 to be validated by the seller's bank server, the buyer's bank server generates payment verification information according to the Bank Credit Certificate Z1 to be validated, and delivers the payment verification information to the client, the client receives the payment verification information input by the buyer and submits it to the buyer's bank server for verification. Wherein, the payment verification information may be a payment page, and the buyer inputs information such as verification information and payment amount on the payment page on the client. The verification information includes at least the bank account number and password, and may further include the verification code, expiration date and other information.

[0073] Specifically, after receiving the Bank Credit Certificate Z1 to be validated, the buyer bank server generates a payment page, and delivers the link address of the payment page to the buyer (for example, delivering the message to the buyer's registered mobile phone). The buyer enters the link address of the payment page on the client or directly clicks the link address received by the client to open the payment page and enters the verification information, payment amount and other payment verification information on the payment page. The buyer's bank server verifies the payment verification information entered by the client on the payment page.

[0074] S15: the buyer's bank server freezes the funds corresponding to the order amount in the buyer's account, and updates the status of the Bank Credit Certificate to the valid status and delivers it to the seller's bank server.

[0075] Specifically, after the verification is passed, the buyer bank server may freeze the corresponding amount of funds in the buyer's account according to the payment amount input

Date Reçue/Date Received 2021-04-20

on the payment page and update the Bank Credit Certificate status, and update the Bank Credit Certificate Z1 to be validated as valid Bank Credit Certificate Z2 and deliver the valid Bank Credit Certificate Z2 to the seller's bank server.

[0076] S16: the seller's bank server updates the status of the valid Bank Credit Certificate to the received certificate and delivers the received certificate to the commodity server.

[0077] In this step S16, after receiving the valid Bank Credit Certificate Z2, the seller's bank server updates the Bank Credit Certificate status, updates the valid Bank Credit Certificate Z2 to the bank credit certificateZ3 that has been validated, and delivers the received card notification to the commodity server.

[0078] S17: the commodity server delivers the order information to the transaction intermediation server according to the received card notification.

[0079] In this step S17, after receiving the commodity receipt notification, the commodity server delivers the order information to the transaction intermediation server.

[0080] S18: the transaction intermediary server arranges the delivery according to the order information, and after determining that the buyer has received the commodity, delivers the receipt notification to the buyer bank server.

[0081] In step S18, after receiving the order information, the transaction intermediation server delivers the commodity according to the transaction information such as the commodity information and the buyer information in the order information. The transaction intermediary server may notify the seller to arrange the delivery, including but not limited to any one or more of the following methods: delivering an email notification to the seller's preset email address, delivering a text message notification to the seller's preset mobile number, deliver the QQ message to the seller's default QQ number, or deliver the WeChat message to the seller's WeChat number presupposed by the seller. The seller will arrange the delivery after receiving the delivery notice.

[0082] After the transaction intermediation server receives the receipt confirmation notification delivered by the client, it determines that the buyer has received the receipt; or the transaction intermediation server does not receive the feedback information of the client within a preset time after the delivery is scheduled, the default buyer has received the commodity after exceeding the preset time. When it is determined that the buyer has received the commodity, the receipt notification is delivered to the buyer's bank server.

[0083] S19: the buyer's bank server transfers the frozen funds in the buyer's account to the seller's

Date Reçue/Date Received 2021-04-20

account of the seller's bank server.

[0084] In this step S19, after the buyer's bank server receives the receipt notification, the frozen funds in the buyer's account are transferred to the seller's account. At this point, the transaction is completed.

[0085] In order to prevent the buyer from receiving the commodity n has not been confirmed receipt, the above method also includes: if the buyer bank server does not receive the notification received by the transaction intermediary server in the preset time, the frozen funds from the buyer's account will be transferred to the seller's account of the seller's Bank after exceeding the preset time.

[0086] By adopting the online transaction method in the above example, the transaction funds and transaction information in the transaction process are not transferred to the third party payment platform, flow within the banking system, this will facilitate the banks to supervise the funds and improve the security of the transaction, at the same time, it is also convenient for banks to supervise the credit of the main body of the transaction, which is beneficial to the establishment of the social credit system. Through the real-time monitoring of transaction status by generating Bank Credit Certificate, there is no deviation between the cash flow time and the actual transaction time, so that the effective flow of no commodity no funds under one line of delivery can effectively reduce the risk of capital and improve the security of transaction information.

[0087] As a preferred example, in order to prevent the transaction information from being stolen, the client, the commodity server, the buyer's bank server, the seller's bank server and the transaction intermediation server use digital envelopes to transmit data and receive data secure transmission. Thereby further enhancing the security of data transmission and ensuring the security of transactions.

[0088] As shown in Figure 3, the data deliverer and data receiver to use digital envelope technology for secure communication data, the specific process is as follows:

[0089] S101: the data deliverer generates a symmetric key, and encrypts the communication data by using a symmetric key to form a first ciphertext.

[0090] In order to prevent the symmetric key from being stolen, the data deliverer randomly generates a symmetric key each time the data is delivered, thereby achieving the effect of dynamic anti-counterfeiting, improving data security, and ensuring transaction security. When encrypting the communication data, the data deliverer preferably encrypts the communication data by using

Date Reçue/Date Received 2021-04-20

the symmetric key to form the first ciphertext.

[0091] S102: the data deliverer encrypts the symmetric key by using the public key of the data receiver to form a second ciphertext.

[0092] S103. The data deliverer signs the first ciphertext and the second ciphertext using its own private key, and delivers the data signature to the data receiver.

[0093] S104: After receiving the first ciphertext and the second ciphertext, the data receiver verifies the signatures of the first ciphertext and the second ciphertext using the public key of the data deliverer.

[0094] S105: After the verification is passed, the data receiver decrypts the second ciphertext using its private key to obtain a symmetric key.

[0095] S106: The data receiver uses the symmetric key to decrypt the first ciphertext to obtain the communication data

[0096] In some examples, the signature step in step S103 and the verification signature step in step S104 may also be omitted.

[0097] Further, in the above examples of the online transaction method, in order to prevent the data from being tampered with after the communication caused by the security of funds, information security and other issues, therefore, the dual-track verification technology is used. Specifically, in the data transmission process, the monitoring server collects the data delivered by the data deliverer and the data received by the data receiver at the same time, verifies the consistency of the data delivered and the received data, and compare the data collected and the received data to determine whether the two are consistent. To further ensure the security of transactions.

[0098] Further, in the online transaction method in the above example, in order to balance the convenience of communication and ensure data security, a dual-network combination technology is adopted. That is, the client, the commodity server, the buyer's bank server and the seller's bank server communicate with each other through the public network, and the monitoring server communicates with the buyer's bank server and the seller's bank server through the private line respectively. As a result it further ensuring the security of the transaction.

[0099] Please refer to Figure 4, a second example of the online transaction method of the present invention is proposed. The method is applied to a commodity server and includes the following steps:

Date Reçue/Date Received 2021-04-20

[0100] S21, after receiving the order information deliver the Bank Credit Certificate issuing request to the seller's Bank server according to the order information.

[0101] Specifically, the Bank Credit Certificate is an electronic certificate promised by a bank, and can be understood as an electronic data that can be stored in a computer system and transmitted through a network. The commodity server is informed of the seller bank servers based on the order information and delivers the Bank Credit Certificate request to the seller bank server.

[0102] S22, after receiving the received card notification delivered by the seller's bank server, deliver the order information to the transaction intermediation server.

[0103] Specifically, after receiving the received certificate notification delivered by the seller bank server, the commodity server delivers the order information to the transaction intermediation server, so that the transaction intermediation server arranges the shipment according to the order information.

[0104] Please refer to Figure 5, a third example of the online transaction method of the present invention is proposed, which is applied to a seller's bank server. The method includes the following steps:

[0105] S31, after receiving the Bank Credit Certificate issuing request delivered by the commodity server, generating a Bank Credit Certificate to be validated and delivering it to the buyer's bank server.

[0106] S32, after receiving the valid Bank Credit Certificate delivered by the buyer's bank server, updating the status of the Bank Credit Certificate to the certified status and delivering the received certificate to the commodity server.

[0107] Please refer to Figure 6, a fourth example of the online transaction method of the present invention is proposed, which is applied to a buyer's bank server. The method includes the following steps:

[0108] S41, after receiving the Bank Credit Certificate of the to-be-validated status delivered by the seller's bank server, acquiring the buyer's payment verification information from the client and performing verification. If the verification is passed, step S602 is executed, otherwise, the flow is ended.

[0109] S42, freezing the funds corresponding to the order amount in the buyer's account, and the status of Bank Credit Certificate is updated to be effective and delivering the status to the seller's bank server.

Date Reçue/Date Received 2021-04-20

[0110] S43. After receiving the received notification delivered by the transaction intermediation server, the frozen funds in the buyer's account are transferred to the seller's account of the seller's bank server.

[0111] Please refer to Figure 7, a fifth example of the online transaction method of the present invention is proposed. The method is applied to an intermediation transaction server and includes the following steps:

[0112] S51, receiving the order information delivered by the commodity server, and arranging the delivery according to the order information.

[0113] Specifically, after receiving the order information, the transaction After receiving the order information, the transaction intermediary server deliver the commodity according to the information of the commodity in the order and the information of the buyer. The transaction intermediary server may notify the seller to arrange the delivery, including but not limited to any one or more of the following methods: delivering an email notification to the seller's preset email address, delivering a text message notification to the seller's preset mobile number, deliver the QQ message to the seller's default QQ number, or deliver the WeChat message to the seller's WeChat number presupposed by the seller. The seller will arrange the delivery after receiving the delivery notice.

[0114] S52. After determining that the buyer has received the commodity, the buyer bank server delivers the commodity receipt notification.

[0115] Specifically, after the transaction intermediation server receives the receipt confirmation notification delivered by the client, it determines that the buyer has received the receipt; or the transaction intermediation server does not receive the feedback information of the client within a preset time after the delivery is scheduled, the default buyer has received the commodity after exceeding the preset time. When it is determined that the buyer has received the commodity, the receipt notification is delivered to the buyer's bank server.

[0116] Please refer to Figure 8, a first example of the online transaction system of the present invention is proposed. The online transaction system in this example is an online transaction system that implements the above online transaction method. The online transaction system includes a client, a commodity server, a buyer Bank server, seller bank server and transaction intermediary server, wherein:

[0117] The client terminal is used to obtain the commodity information from the commodity server, generate the order according to the commodity ordered by the buyer, and deliver the order to

Date Reçue/Date Received 2021-04-20

the commodity server; after receiving the payment verification request delivered by the buyer bank server, deliver the payment check information for the buyer's input to the buyer's bank server.

[0118] Wherein, please refer to Figure 9, an online transaction device applied to a client includes the following modules:

[0119] An order delivery module is used to obtain commodity information from the commodity server, generate an order based on the commodity ordered by the buyer, and deliver the order to the commodity server;

[0120] The verification information delivery module is used to deliver the payment verification information input by the buyer to the buyer's bank server after receiving the payment verification request delivered by the buyer's bank server.

[0121] The commodity server: after receiving the order information delivered by the client, delivers a request for issuing a Bank Credit Certificate to the seller's bank server, and also receives the received certificate notification delivered by the seller's bank server, and it is also set to deliver the order information to the transaction intermediary server after receiving the received notice from the seller's bank server.

[0122] Please refer to Figure 10, an online trading device applied to a commodity server includes the following modules:

[0123] The first receiving module is used to receive the order information delivered by the client and the received card notification delivered by the seller's bank server;

[0124] The issuing request module is used to deliver a Bank Credit Certificate issuing request to the seller's bank server according to the order information after receiving the order information delivered by the client;

[0125] The order information delivery module is used to deliver the order information to the transaction intermediation server after receiving the received card notification delivered by the seller's bank server.

[0126] The seller bank server is used to generate a Bank Credit Certificate of the to-be-validated state after receiving the Bank Credit Certificate issuing request and deliver the Bank Credit Certificate to the buyer bank server; and after receiving the effective Bank Credit Certificate delivered to the buyer bank server, the status of the Bank Credit Certificate is updated to the accepted status, and the received notification is delivered to the commodity server;

[0127] Wherein, refer to Figure 11, the online trading device applied to the seller's bank server

Date Reçue/Date Received 2021-04-20

includes the following modules:

[0128] A second receiving module is used to receive a Bank Credit Certificate issuing request delivered by the commodity server and an effective Bank Credit Certificate delivered by the buyer's bank server;

[0129] Bank Credit Certificate generating module is used to generate a Bank Credit Certificate which is in effect according to a Bank Credit Certificate issuing request;

[0130] The Bank Credit Certificate delivery module is used to deliver the Bank Credit Certificate to be validated to the buyer bank server;

[0131] The received module notification module is used to receive the Bank Credit Certificate valid from the first bank server, update the status of the Bank Credit Certificate to the certified status, and deliver the received certificate to the commodity server.

[0132] The buyer's bank server: set to receive the Bank Credit Certificate delivered by the seller's bank server to be validated, acquires the buyer's payment verification information from the client and performs verification; if the verification is successful, the buyer's account corresponding to the order amount is frozen and update the status of the Bank Credit Certificate to the valid status and deliver it to the seller bank server; After receiving the received notification delivered by the transaction intermediary server, the user is also allowed to transfer the frozen funds by the buyer's account to the seller's account of the seller's bank server.

[0133] Wherein, please refer to Figure 12, the online trading device applied to the buyer's bank server includes the following modules:

[0134] A third receiving module is used to receive a Bank Credit Certificate delivered by the seller's bank server and to be validated and a receipt notification delivered by the transaction intermediation server;

[0135] The verification module is used to after receiving the Bank Credit Certificate delivered by the second bank server to be validated, obtain the buyer's payment verification information from the client and perform verification;

[0136] The freezing module is used to freeze the funds corresponding to the order amount in the buyer's account after the verification is passed, and update the status of the Bank Credit Certificate to be valid and deliver it to the seller's bank server;

[0137] The money transfer module is used to, after receiving the received notification delivered by the transaction intermediation server, the frozen funds in the buyer's account are transferred to

Date Reçue/Date Received 2021-04-20

the seller's account of the seller's bank server.

[0138] In order to prevent the buyer does not confirm receipt of commodity after receiving the commodity, and the money transfer module is also used: If no receiving notification is received from the transaction intermediation server within the preset time, then after a preset time, the funds frozen by the buyer's account are transferred to the seller's account of the seller bank server.

[0139] The transaction intermediation server is used to receive order information delivered by the commodity server, arrange delivery according to the order information, and deliver a receipt notification to the buyer's bank server after determining that the buyer has received the commodity.

[0140] Wherein, please refer to Figure 13, an online transaction device applied to a transaction intermediation server includes the following modules:

[0141] A fourth receiving module is used to receive the order information delivered by the commodity server;

[0142] The delivery scheduling module is used to arrange delivery according to the transaction information such as commodity information, buyer information and so on in the order information; specifically, the seller may notify the seller to arrange the delivery, including but not limited to any one or more of the following methods: delivering an email notification to the seller's preset email address, delivering a text message notification to the seller's preset mobile number, deliver the QQ message to the seller's default QQ number, or deliver the WeChat message to the seller's WeChat number presupposed by the seller. The seller will arrange the delivery after receiving the delivery notification;

[0143] The received notification module is used to deliver a receipt notification to the buyer's bank server after determining that the buyer has received the commodity. Specifically, after the receiving notification module receives the receiving confirmation notification delivered by the client, it determines that the buyer has received the commodity; or, the receiving notification module does not receive feedback from the client within a preset time after arranging the shipment, and the buyer has received the commodity by default after the preset time.

[0144] Specifically, the seller stores the commodity information in the commodity server, and the buyer communicates with the commodity server through the client, acquires the commodity information from the commodity server, and selects the commodity that needs to be purchased. The client generates order information according to the commodity information selected by the

Date Reçue/Date Received 2021-04-20

buyer and submits the order information to the commodity server. Wherein, the commodity includes tangible physical commodity and invisible services. The commodity information includes commodity price, parameters and so on. The commodity server may be a commercial computer server or a seller's own computer server. The client is a communication terminal operated by the buyer, including but not limited to terminal devices such as mobile phones, tablet devices and computers. The buyer's bank server refers to the bank server where the buyer's bank account is located and the seller bank server refers to the bank server where the seller's bank account is located. The buyer bank server and the seller bank server may be servers of the same bank (i.e. the buyer and the seller's bank account are same), may also be different bank server (that is, the buyer and the seller's bank are not at the same time). Bank Credit Certificate is an electronic certificate that a bank promises to pay for. It can be understood as an electronic data that can be stored in a computer system and transmitted over the Internet.

[0145] With the online trading system of this example, transaction funds and transaction information in the transaction process are not transferred to a third-party payment platform, and the status of the transaction is monitored in real time by generating a Bank Credit Certificate, so that there is no deviation between the time of capital flow and the actual transaction time, so that the effective delivery of cash flow can effectively reduce the financial risk and improve the security of transaction information.

[0146] As a preferred example, in order to prevent the transaction information from being stolen, the client, the commodity server, the seller's bank server, the buyer's bank server and the transaction intermediation server are also used in the data delivering and receiving, the digital envelope technology is used to transmit the communication data safely. Thereby further enhancing the security of data transmission and ensuring the security of transactions.

[0147] When the client, the commodity server, the seller's bank server, the buyer's bank server and the transaction intermediation server serve as the data deliverer, it is also set as follows:

[0148] Generating a first ciphertext by using a symmetric key, encrypting the symmetric key by using a public key of the data receiving party, and forming a second ciphertext by using a public key of the data receiver; a ciphertext and the second ciphertext are signed and delivered to the data receiver.

[0149] In order to further prevent the symmetric key from being stolen, each time the data deliverer delivers data, a symmetric key is dynamically generated at random, so as to achieve the effect

Date Reçue/Date Received 2021-04-20

of dynamic anti-counterfeiting. When encrypting the communication data, the data deliverer preferably encrypts the communication data by using the symmetric key to form the first ciphertext.

[0150] When the client, the commodity server, the seller bank server buyer bank server and the intermediary transaction server serve as the data deliverer, it is also set as follows:

[0151] After receiving the first ciphertext and the second ciphertext, the signature of the first ciphertext and the second ciphertext are verified by using the public key of the deliverer of the data; when the verification is passed, the symmetric key is obtained by using its own private key to decrypt the second ciphertext, and the communication data is obtained by using the symmetric key to decrypt the first ciphertext.

[0152] In some examples, the data deliverer may not sign the first ciphertext and the second ciphertext, and the corresponding data receiver does not need to perform signature verification on the first ciphertext and the second ciphertext.

[0153] Please refer to Figure 14, a second example of the online transaction system of the present invention is proposed. The difference between this example and the first example is that a monitoring server is added, and the monitoring server is used to:

[0154] During the data transmission, the data delivered by the data deliverer and the data received by the data receiver are collected at the same time, verifies the consistency of the data delivered and the received data, and compare the data collected and the received data to determine whether the two are consistent. Wherein, the client, the commodity server, the seller bank server, the buyer bank server and the transaction intermediary server are the data delivering parties when delivering data, they are the data deliver and the data receiver when they receive the data. Therefore, the present example uses a dual-track verification technology to prevent data from being tampered with during communications and further ensure transaction security.

[0155] Further, in order to balance the convenience of communication and ensure data security, this example also uses a combination of two networks. That is, the client, the commodity server, the buyer's bank server and the seller's bank server communicate with each other through the public network, and the monitoring server communicates with the buyer's bank server and the seller's bank server through the private line respectively. To further ensure the security of transactions.

[0156] It should be noted that, the technical features in the foregoing method examples are applicable to both the system and device examples, and are not described again here.

Date Reçue/Date Received 2021-04-20

[0157] A person of skill in the art considers the problems disclosed herein and sought to be solved by the present disclosure to be exclusively computer problems and contemplates only solutions to those problems that include essential computer elements. Abstract ideas, mere schemes, plans, rules, or mental processes that do not include computer elements are expressly excluded from this application.

[0158] A person of skill in the art will understand that the realization of all or part of the steps of the method described above may be controlled by a program to control the associated hardware completion, which may be stored in a computer-readable storage medium. The storage medium may be ROM / RAM, a magnetic disk, an optical disk, etc.

[0159] It is to be understood that the above is only a preferred example of the present invention and is not intended to limit the scope of the invention as a matter of limitation, either by way of equivalent construction or equivalent process transformation using the present specification and the accompanying drawings, directly or indirectly used in other related technical fields, which are included in the scope of the patent protection of the present invention.

Industrial utility

[0160] The online transaction method, device and system of the present invention deliver the issuing request to the seller's bank server through the commodity server, the intermediary transaction server delivers the receiving notification to the buyer's bank server, the client, the commodity server, the buyer's bank server, the seller's bank server and the transaction intermediary server to complete the transaction process, the transaction process of transaction funds, transaction information does not go to the third-party payment platform, and all flow within the banking system, it is convenient for the bank to supervise the capital and the subject's credit supervision. And the transaction status is monitored in real time by generating Bank Credit Certificate so that there is no deviation between the time of fund flow and the actual transaction time, so that it can effectively reduce the risk of funds and improve the security of the transaction information. In addition, the use of digital envelopes and dynamic anti-counterfeiting technology for secure transmission of communication data to ensure the safety of communication data; the use of double-track check to prevent data from being tampered with technology; the two networks are used to balance the convenience and security of communication.

Date Reçue/Date Received 2021-04-20

Claims:

1. A computer implemented method for online transaction, applied in a buyer's bank server, the method comprising:

   receiving a to-be-validated Bank Credit Certificate generated by a seller's bank server;

   acquiring buyer's payment verification information from a client device to perform a verification process;

   freezing an amount of funds in a buyer's account corresponding to an amount of funds in an order when the verification process is passed;

   updating status of a Bank Credit Certificate to a validated status and delivering the validated status for the Bank Credit Certificate to the seller's bank server; and

   unfreezing a frozen amount of funds in the buyer's account to transfer the amount of funds to a seller's account through the seller's bank server, after receiving a receipt notification for commodity delivery from a transaction intermediation server.

2. The method of claim 1, wherein the Bank Credit Certificate is configured as data that may be stored in a computer system and transmitted via the Internet.

3. The method of claim 1 further includes transmitting communicative data to the client device, the transaction intermediation server and the seller's bank server respectively via digital envelopes for data security.

4. The method of claim 2, wherein transmitting communicative data via digital envelopes for data security further includes that

Date Reçue/Date Received 2022-08-22

a data sender generates a symmetric key and encrypts the communicative data by using the symmetric key to form a first ciphertext, as well as by using a public key of the data receiver to encrypt the symmetric key to form a second ciphertext, then the data sender delivers the first ciphertext and the second ciphertext to a data receiver; and

the data receiver decrypts the second ciphertext by using an own private key to obtain the symmetric key and decrypts the first ciphertext by using the symmetric key to obtain the communicative data.

5. The method of claim 4 further includes that

the data deliverer signs digitally the first ciphertext and the second ciphertext respectively by using the own private key; and

the data receiver verifies the first ciphertext and the second ciphertext with the digital signs respectively by using the public key from the data deliverer.

6. The method of claim 4, wherein the data sender randomly generates the symmetric key dynamically.

7. The method of claim 4, wherein the data sender encrypts the communicative data by using the symmetric key based on an Advanced Encryption Standard (AES) algorithm to form the first ciphertext.

8. The method of any one of claims 1 to 7, wherein the client device is configured as the data sender when sending the communicative data.

9. The method of any one of claims 1 to 7, wherein the buyer's bank server is configured as the data sender when sending the communicative data.

Date Reçue/Date Received 2022-08-22

10. The method of any one of claims 1 to 7, wherein the buyer's bank server is configured as the data receiver when receiving the communicative data.

11. The method of any one of claims 1 to 7, wherein the seller's bank server is configured as the data sender when sending the communicative data.

12. The method of any one of claims 1 to 7, wherein the seller's bank server is configured as the data receiver when receiving the communicative data.

13. The method of any one of claims 1 to 7, wherein the transaction intermediation server is configured as the data sender when sending the communicative data.

14. The method of any one of claims 2 to 12, wherein the communicative data is transmitted among the client device, a commodity server, the buyer's bank server and the seller's bank server through a public network.

15. The method of any one of claims 2 to 14, wherein the communicative data is transmitted among a monitoring server, the buyer's bank server, and the seller's bank server via dedicated line communication.

16. The method of any one of claims 1 to 15, wherein the buyer's bank server is configured as a computer server corresponding to the buyer's bank account.

17. The method of any one of claims 1 to 15, wherein the seller's bank server is configured as a computer server corresponding to the seller's bank account.

18. The method of any one of claims 1 to 17, wherein the seller's bank server and the buyer's bank server may be the same.

19. The method of any one of claims 1 to 17, wherein the seller's bank server is different from the buyer's bank server.

Date Reçue/Date Received 2022-08-22

20. The method of any one of claims 1 to 19, wherein the payment verification information is a webpage for payment.

21. The method of claim 20, wherein the webpage for payment is configured to be inputted verification information by the buyer via the client device.

22. The method of any one of claims 20 to 21, wherein the verification information includes buyer's bank account number.

23. The method of any one of claims 1 to 22, wherein the verification information includes password of the buyer's bank account.

24. The method of any one of claims 1 to 23, wherein the verification information includes verification code.

25. The method of any one of claims 1 to 24, wherein the verification information includes expiration date.

26. The method of any one of claims 1 to 25, wherein the webpage for payment is configured to be inputted payment amount by the buyer via the client device.

27. A computer device for online transaction, applied in a buyer's bank server, the device comprising:

a third receiving module configured to:

receive a to-be-validated Bank Credit Certificate generated by a seller's bank server; and

Date Reçue/Date Received 2022-08-22

receive a receipt notification for commodity delivery from a transaction intermediation server;

a verification module configured to acquire buyer's payment verification information from a client device to perform a verification process;

a freezing module configured to:

freeze an amount of funds in a buyer's account corresponding to an amount of funds in an order when the verification process is passed; and

update status of a Bank Credit Certificate to a validated status and delivering the validated status for the Bank Credit Certificate to the seller's bank server;

a money transfer module configured to unfreeze a frozen amount of funds in the buyer's account to transfer the amount of funds to a seller's account through the seller's bank server, after receiving a receipt notification for commodity delivery from the transaction intermediation server.

28. The device of claim 27, wherein the Bank Credit Certificate is configured as data that may be stored in a computer system and transmitted via the Internet.

29. The device of claim 27, wherein the third receiving module is further configured to transmit communicative data with the client device, the transaction intermediation server and the seller's bank server respectively via digital envelopes for data security.

30. The device of claim 27, wherein the verification module is further configured to transmit communicative data with the client device via digital envelopes for data security.

31. The device of claim 27, wherein the freezing module is further configured to transmit communicative data with the seller's bank server via digital envelopes for data security.

Date Reçue/Date Received 2022-08-22

32. The device of claim 27, wherein the money transfer module is further configured to transmit communicative data with the seller's bank server via digital envelopes for data security.

33. The device of any one of claims 28 to 32, wherein transmitting communicative data via digital envelopes for data security further includes that

a data sender generates a symmetric key and encrypts the communicative data by using the symmetric key to form a first ciphertext, as well as by using a public key of the data receiver to encrypt the symmetric key to form a second ciphertext, then the data sender delivers the first ciphertext and the second ciphertext to a data receiver; and

the data receiver decrypts the second ciphertext by using an own private key to obtain the symmetric key and decrypts the first ciphertext by using the symmetric key to obtain the communicative data.

34. The device of claim 33 further includes that

the data deliverer signs digitally the first ciphertext and the second ciphertext respectively by using the own private key; and

the data receiver verifies the first ciphertext and the second ciphertext with the digital signs respectively by using the public key from the data deliverer.

35. The device of claim 33, wherein the data sender randomly generates the symmetric key dynamically.

36. The device of claim 33 wherein the data sender encrypts the communicative data by using the symmetric key based on an Advanced Encryption Standard (AES) algorithm to form the first ciphertext.

Date Reçue/Date Received 2022-08-22

37. The device of any one of claims 27 to 36, wherein the client device is configured as the data sender when sending the communicative data.

38. The device of any one of claims 27 to 36, wherein the transaction intermediation server is configured as the data sender when sending the communicative data.

39. The device of any one of claims 27 to 36, wherein the buyer's bank server is configured as the data sender when sending the communicative data.

40. The device of any one of claims 27 to 36, wherein the buyer's bank server is configured as the data receiver when receiving the communicative data.

41. The device of any one of claims 27 to 36, wherein the seller's bank server is configured as the data sender when sending the communicative data.

42. The device of any one of claims 27 to 36, wherein the seller's bank server is configured as the data receiver when receiving the communicative data.

43. The device of any one of claims 28 to 36, wherein the communicative data is transmitted among the client device, a commodity server, the buyer's bank server and the seller's bank server through a public network.

44. The device of any one of claims 28 to 36, wherein the communicative data is transmitted among a monitoring server, the buyer's bank server, and the seller's bank server via dedicated line communication.

45. The device of any one of claims 27 to 44, wherein the buyer's bank server is configured as a computer server corresponding to the buyer's bank account.

46. The device of any one of claims 27 to 45, wherein the seller's bank server is configured as a computer server corresponding to the seller's bank account.

Date Reçue/Date Received 2022-08-22

47. The device of any one of claims 27 to 46, wherein the seller's bank server and the buyer's bank server may be the same.

48. The device of any one of claims 27 to 46, wherein the seller's bank server is different from the buyer's bank server.

49. The device of any one of claims 27 to 48, wherein the payment verification information is a webpage for payment.

50. The device of claim 49, wherein the webpage for payment is configured to be inputted verification information by the buyer via the client device.

51. The device of any one of claims 49 to 50, wherein the verification information includes buyer's bank account number.

52. The device of any one of claims 27 to 51, wherein the verification information includes password of the buyer's bank account.

53. The device of any one of claims 27 to 52, wherein the verification information includes verification code.

54. The device of any one of claims 27 to 53, wherein the verification information includes expiration date.

55. The device of any one of claims 27 to 54, wherein the webpage for payment is configured to be inputted payment amount by the buyer via the client device.

Date Reçue/Date Received 2022-08-22

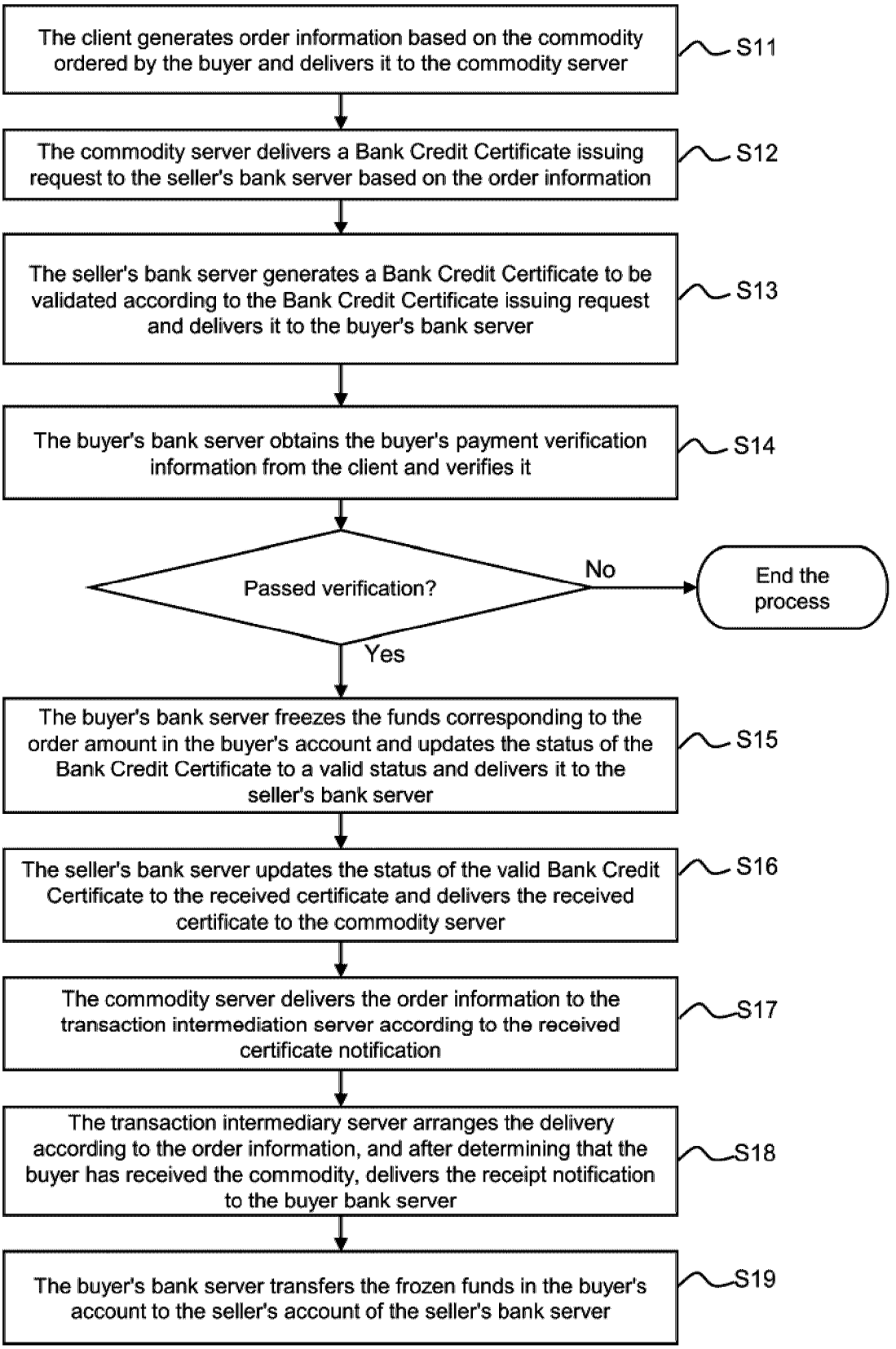


Figure 1

Date reçue / Date received 2021-12-16

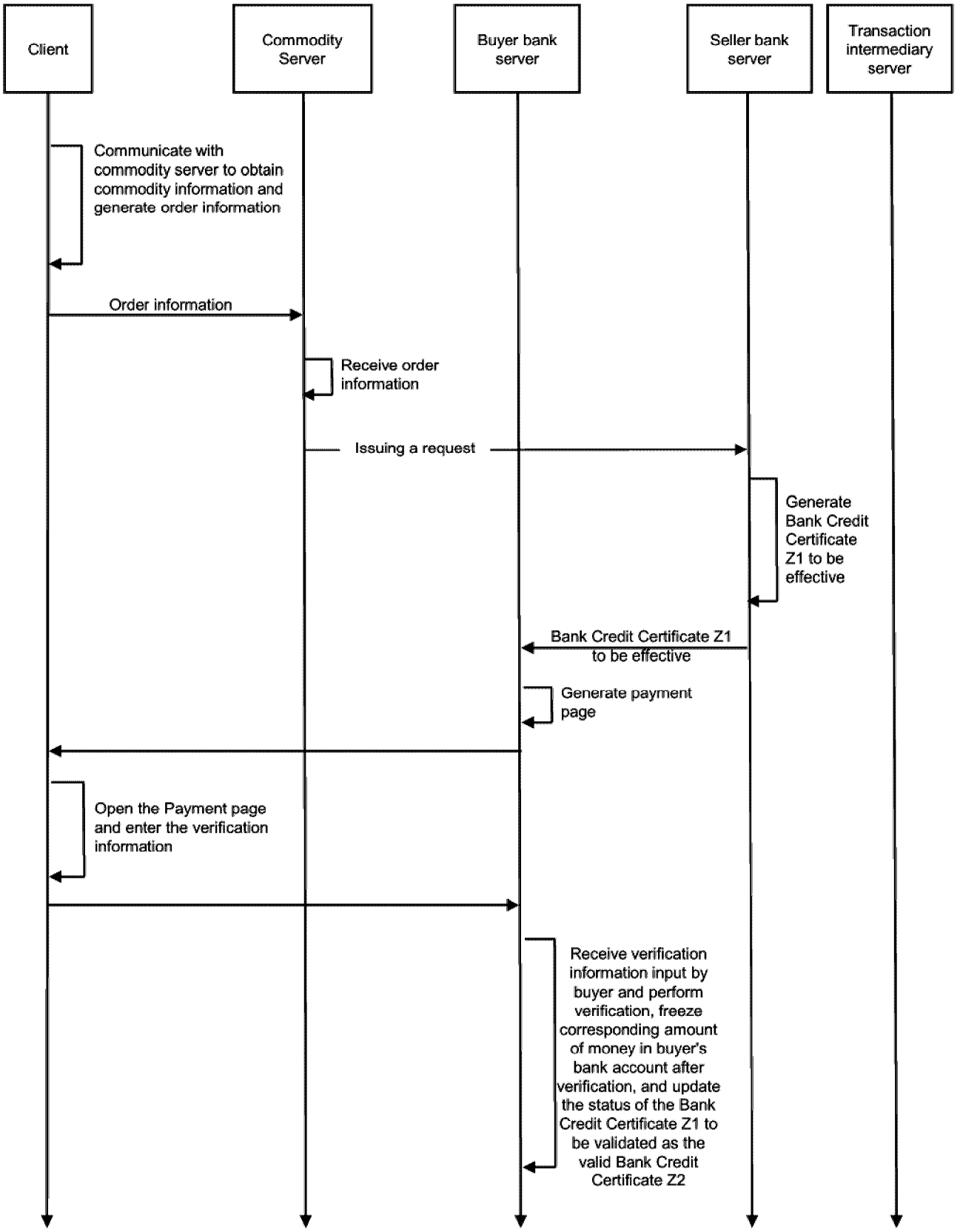


Figure 2a

Date reçue / Date received 2021-12-16

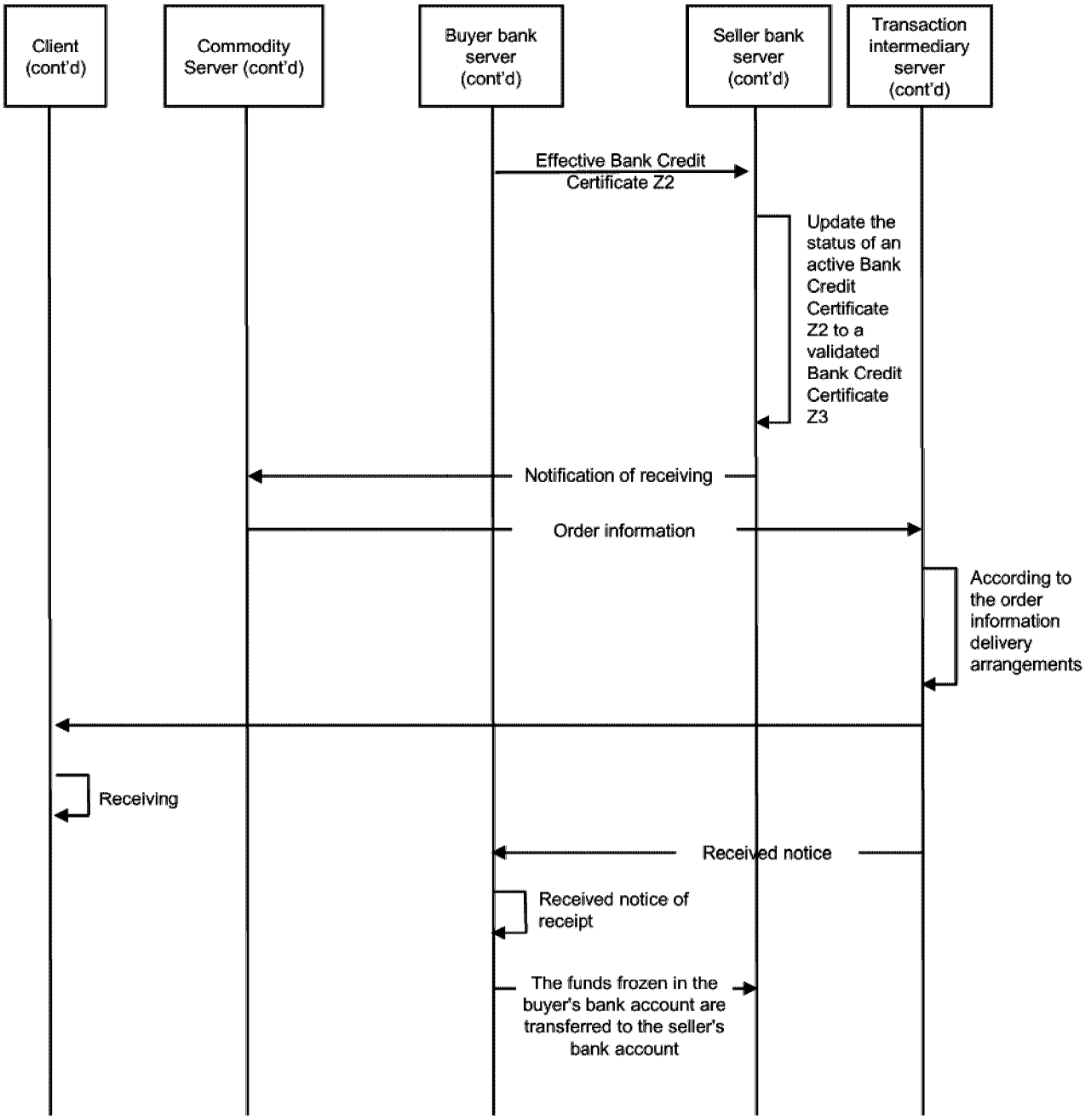


Figure 2b

Date reçue / Date received 2021-12-16

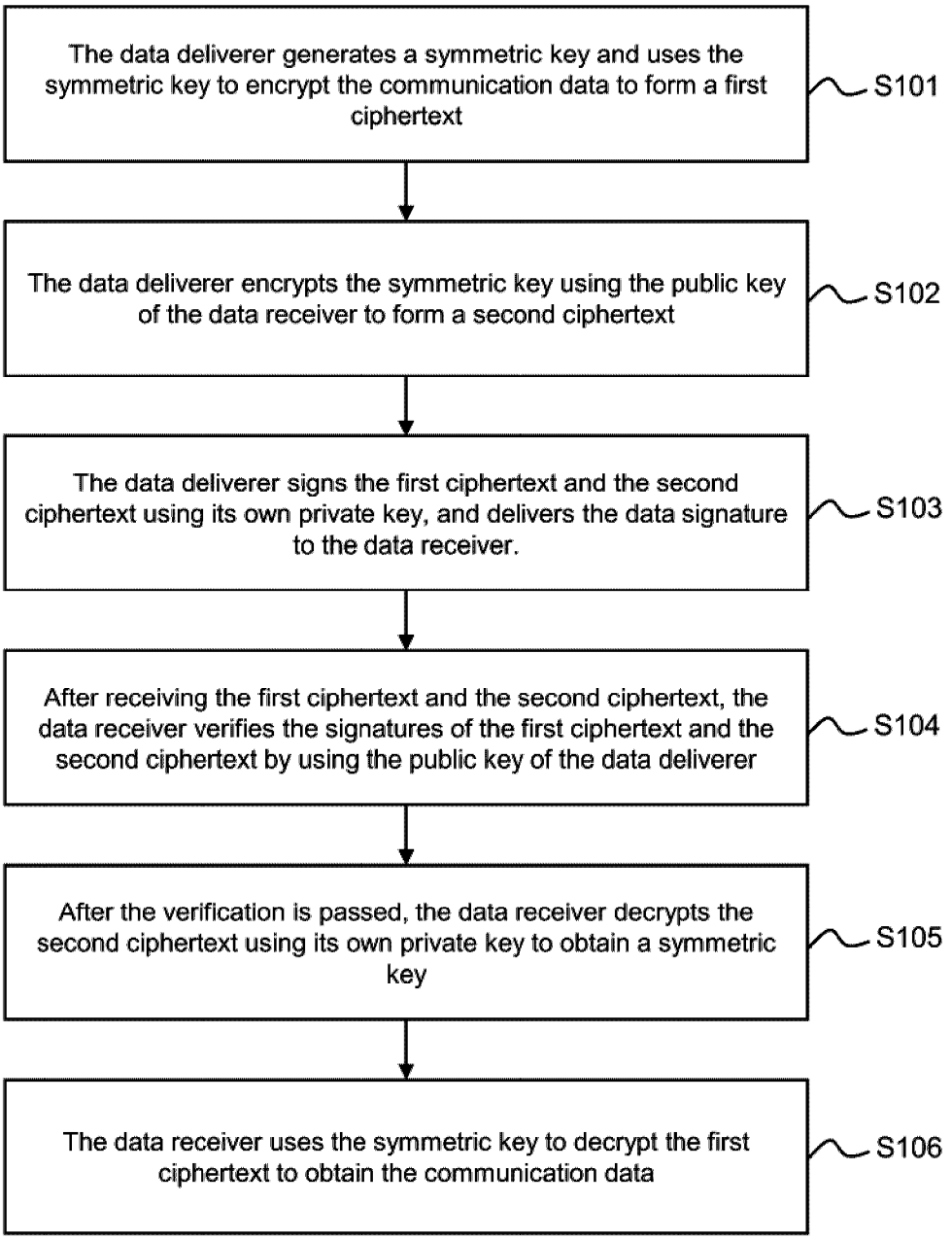


Figure 3

Date reçue / Date received 2021-12-16

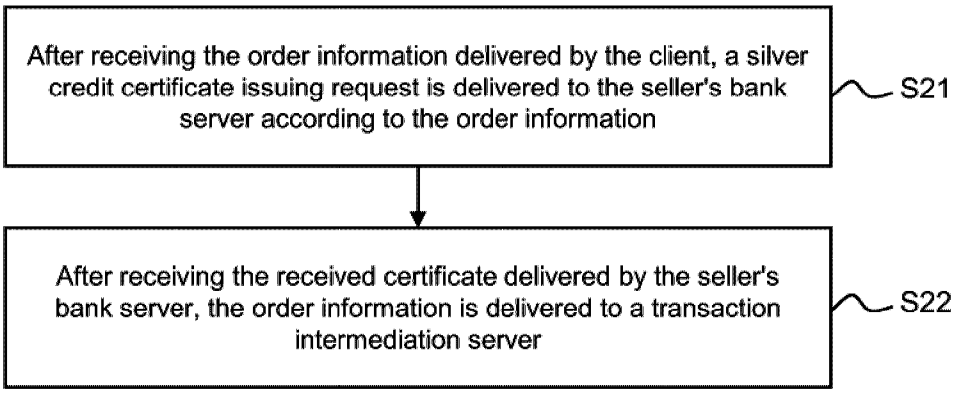


Figure 4

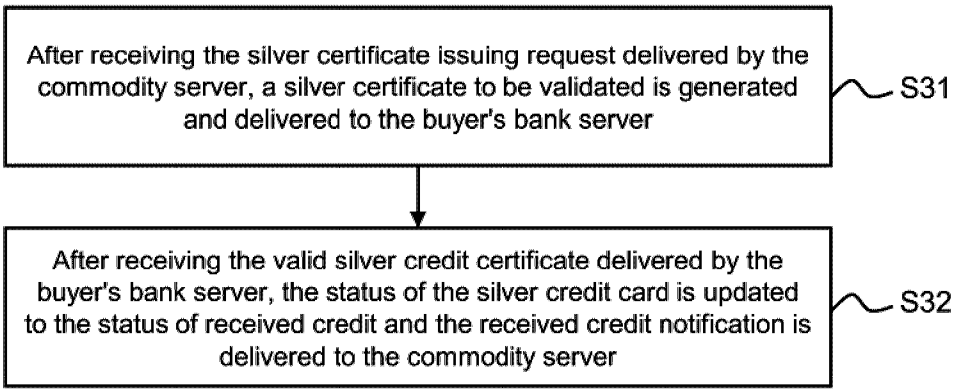


Figure 5

Date reçue / Date received 2021-12-16

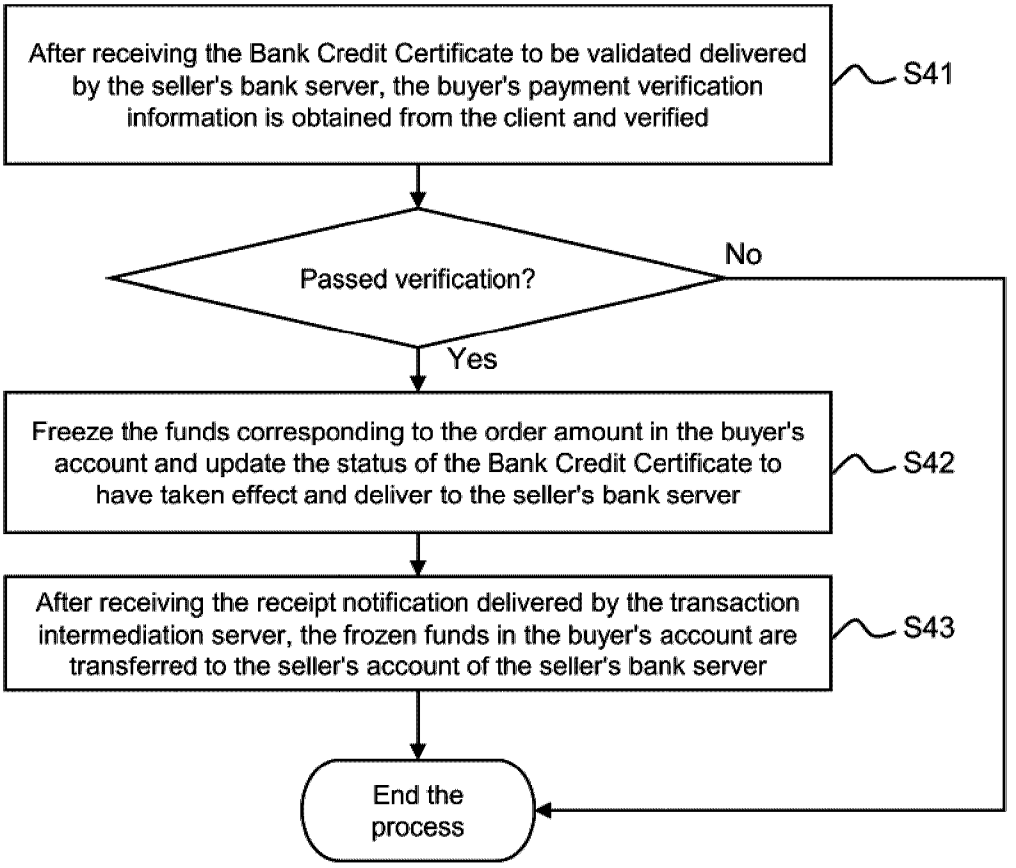


Figure 6

Date reçue / Date received 2021-12-16

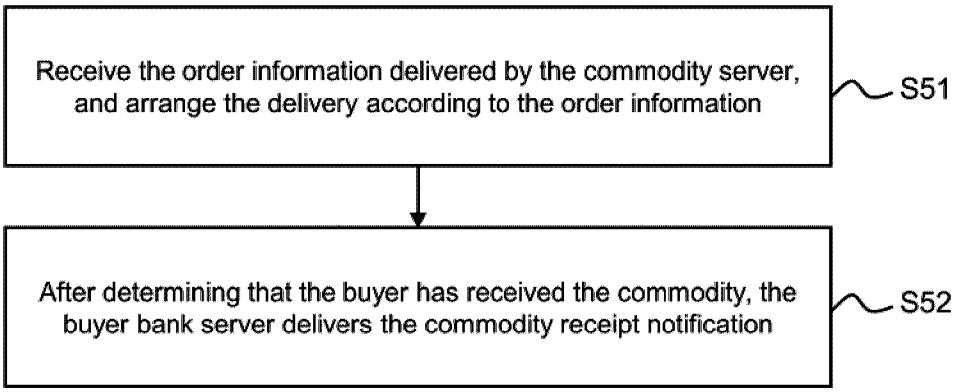


Figure 7

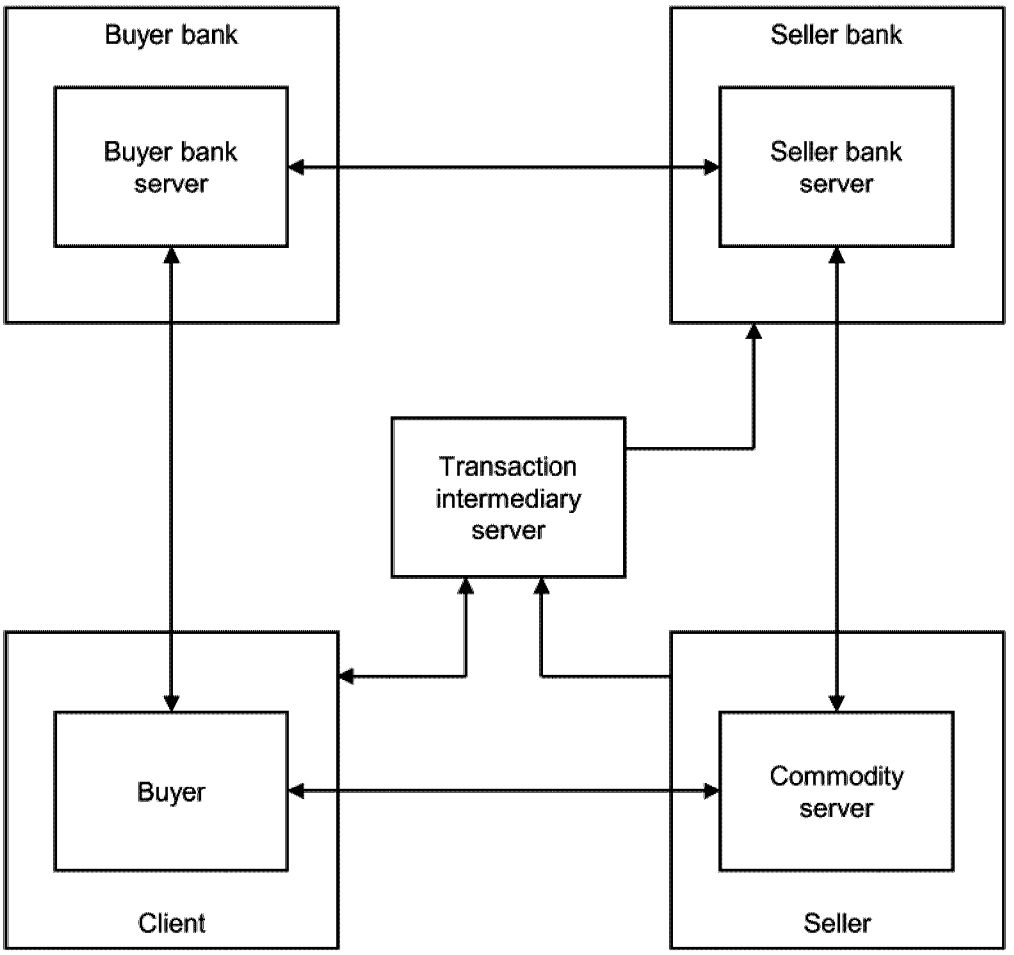


Figure 8

Date reçue / Date received 2021-12-16

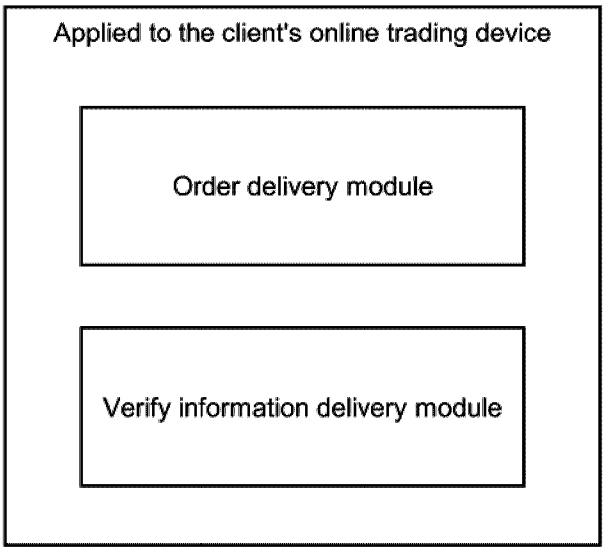


Figure 9

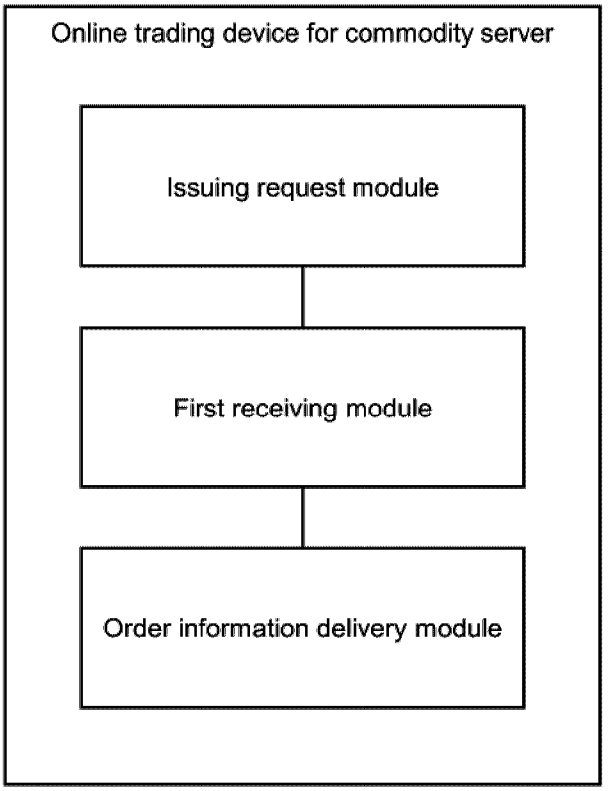


Figure 10

Date reçue / Date received 2021-12-16

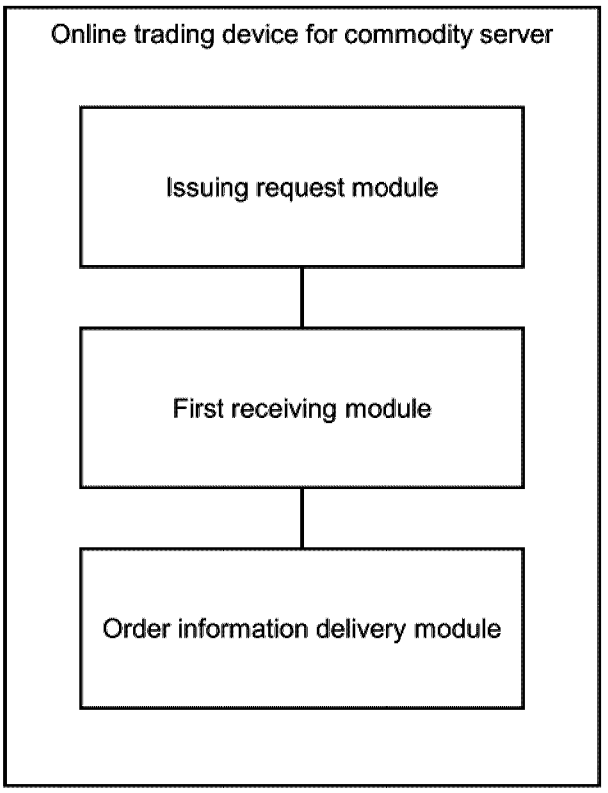


Figure 10

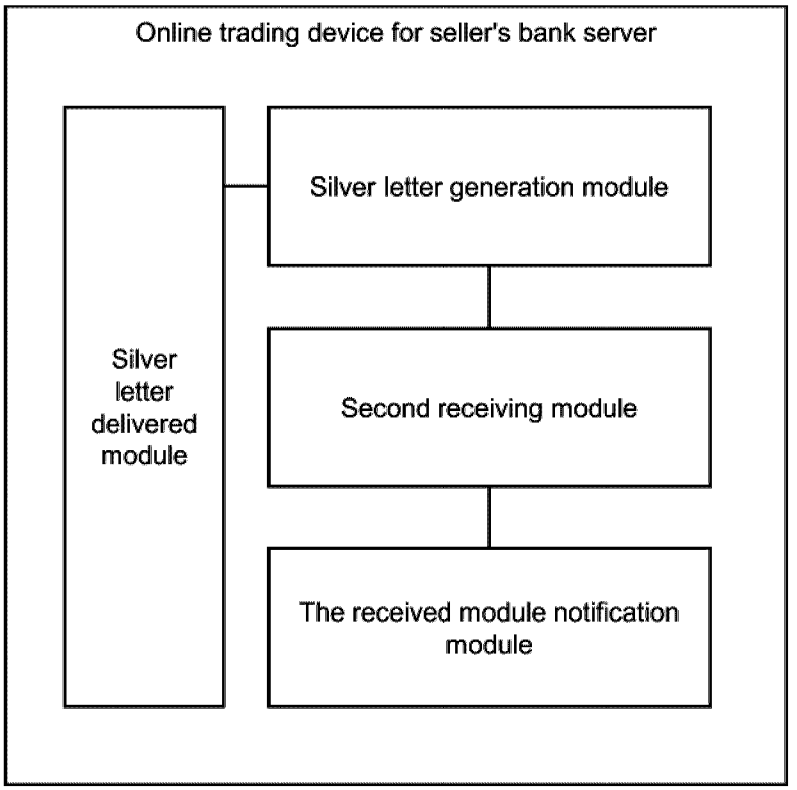


Figure 11

Date reçue / Date received 2021-12-16

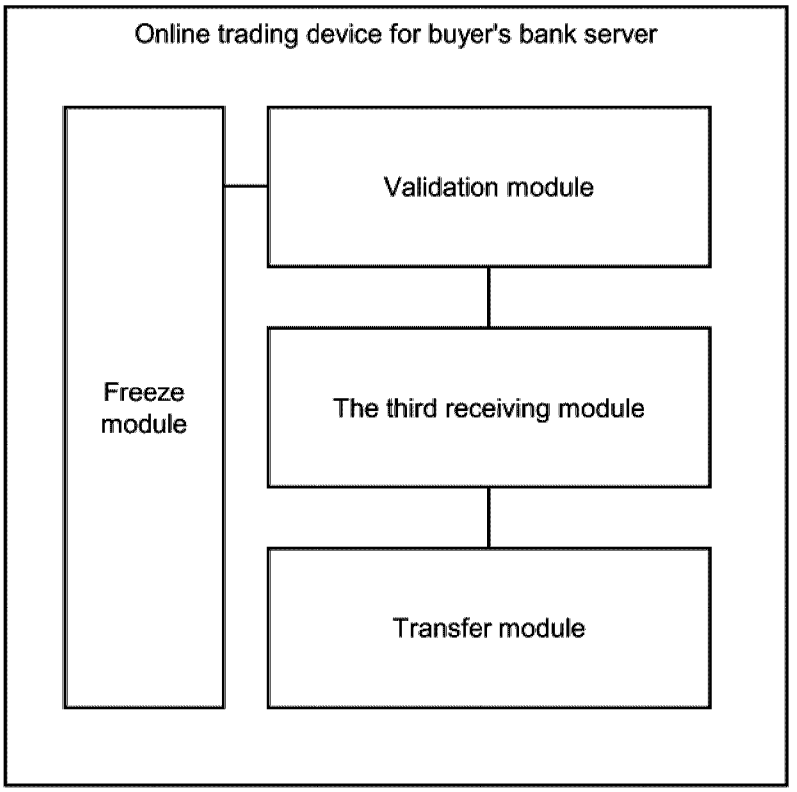


Figure 12

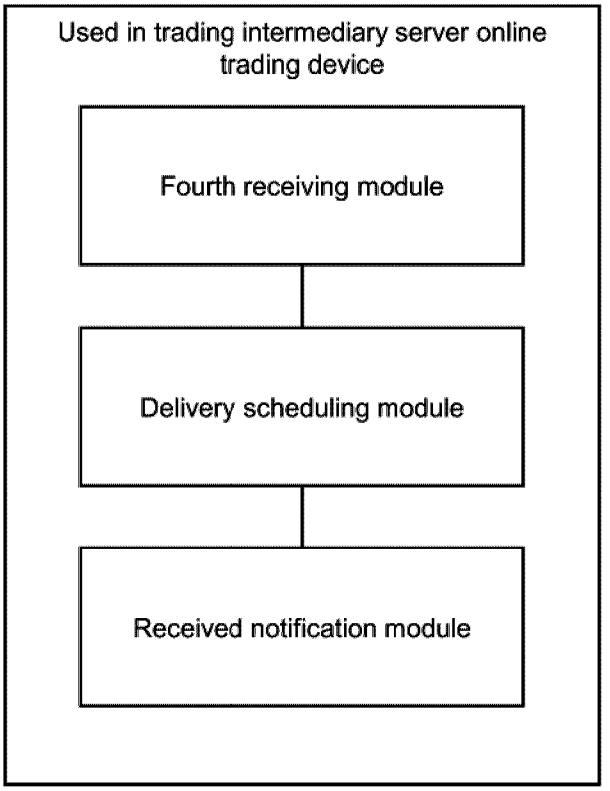


Figure 13

Date reçue / Date received 2021-12-16

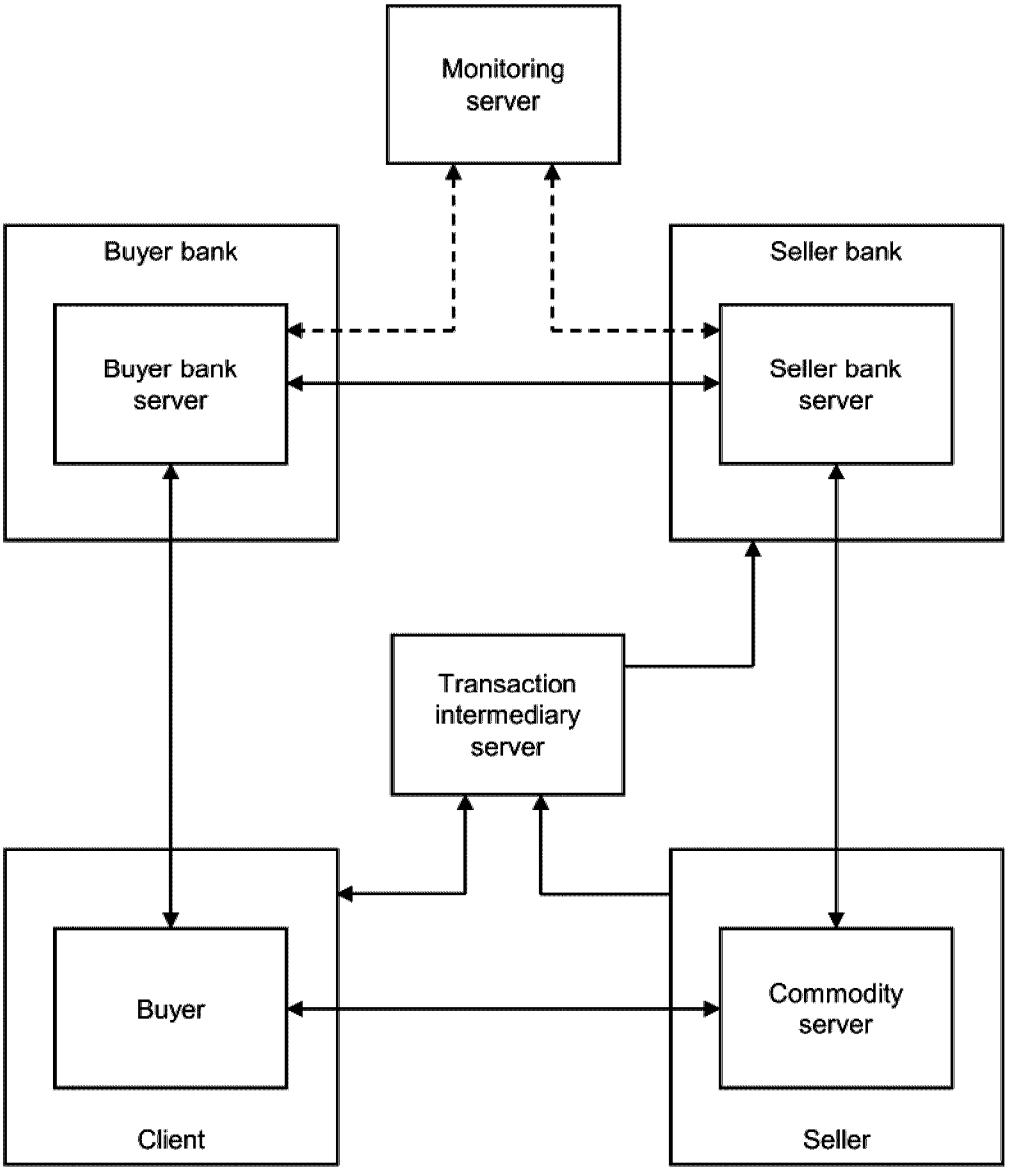
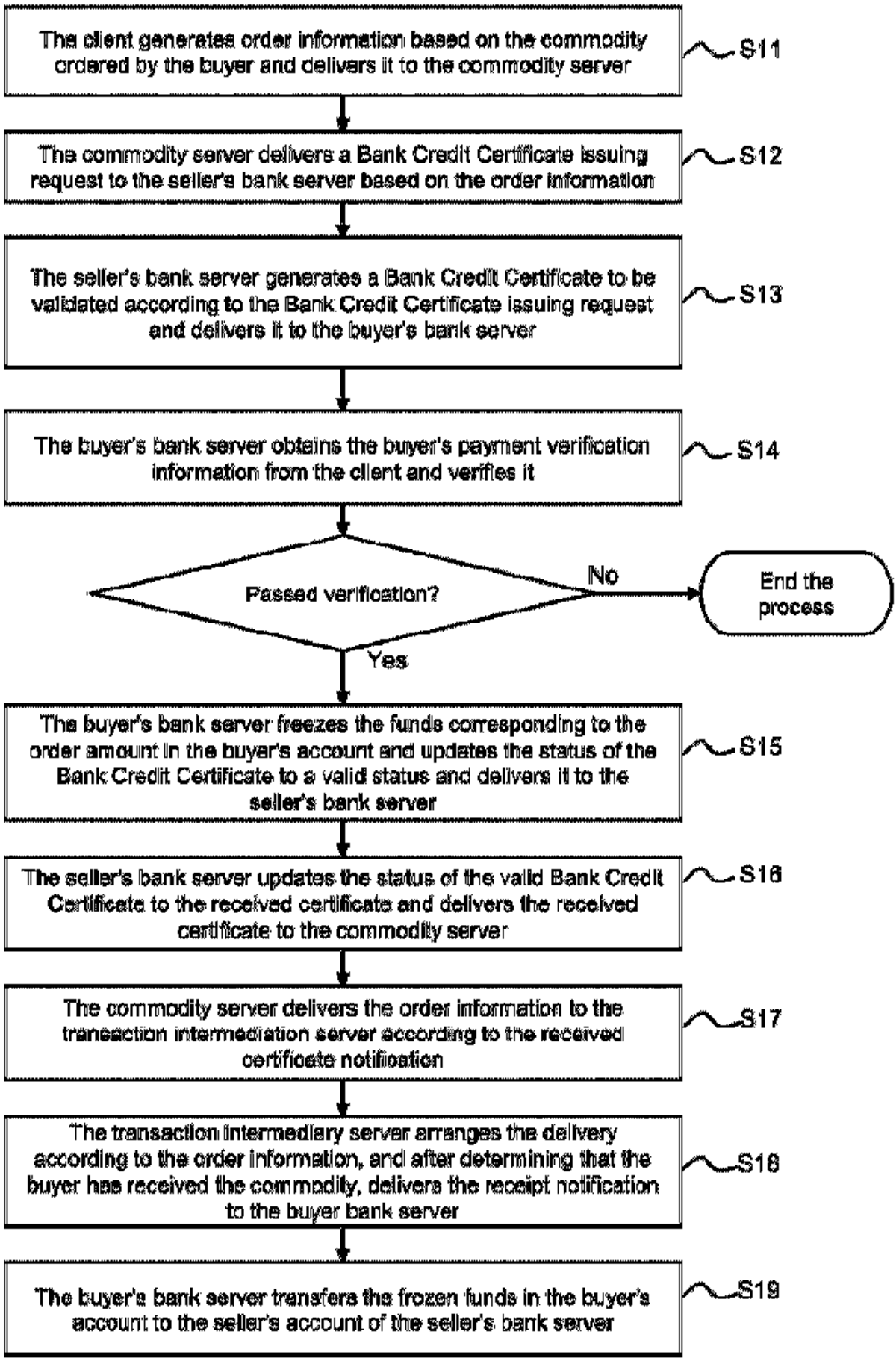


Figure 14

Date reçue / Date received 2021-12-16


The client generates order information based on the commodity ordered by the buyer and delivers it to the commodity server
S11
The commodity server delivers a Bank Credit Certificate issuing request to the seller's bank server based on the order information
S12
The seller's bank server generates a Bank Credit Certificate to be validated according to the Bank Credit Certificate issuing request and delivers it to the buyer's bank server
S13
The buyer's bank server obtains the buyer's payment verification information from the client and verifies it
S14
Passed verification?
No
End the process
Yes
The buyer's bank server freezes the funds corresponding to the order amount in the buyer's account and updates the status of the Bank Credit Certificate to a valid status and delivers it to the seller's bank server
S15
The seller's bank server updates the status of the valid Bank Credit Certificate to the received certificate and delivers the received certificate to the commodity server
S16
The commodity server delivers the order information to the transaction intermediation server according to the received certificate notification
S17
The transaction intermediary server arranges the delivery according to the order information, and after determining that the buyer has received the commodity, delivers the receipt notification to the buyer bank server
S18
The buyer's bank server transfers the frozen funds in the buyer's account to the seller's account of the seller's bank server
S19