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

Innovation, Science and Economic Development Canada
Canadian Intellectual Property Office

CA 2993087 C 2023/02/07

(11)(21) **2 993 087**

(12) **BREVET CANADIEN**
CANADIAN PATENT

(13) **C**

(86) **Date de dépôt PCT/PCT Filing Date:** 2015/07/21
(87) **Date publication PCT/PCT Publication Date:** 2017/01/26
(45) **Date de délivrance/Issue Date:** 2023/02/07
(85) **Entrée phase nationale/National Entry:** 2018/01/19
(86) **N° demande PCT/PCT Application No.:** CN 2015/084660
(87) **N° publication PCT/PCT Publication No.:** 2017/012063

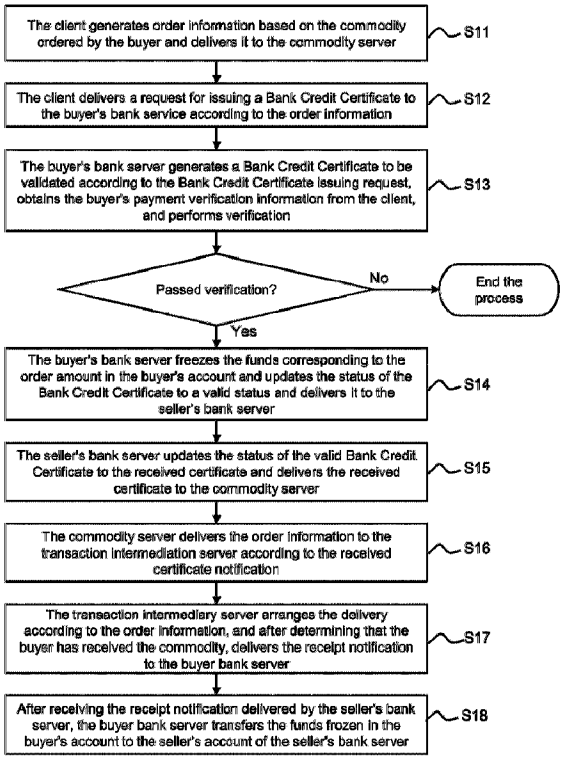
(51) **Cl.Int./Int.Cl.** ***G06Q 20/12*** (2012.01)

(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: a client generates order information according to an item ordered by a buyer, and sends the order information to an item server; the client sends a bank

CA 2993087 C 2023/02/07

(11)(21) 2 993 087

(13) C

(57) **Abrégé(suite)/Abstract(continued):**
credit certificate issuing request to a buyer bank server; the buyer bank server generates a bank credit certificate having a to-be-effective status, 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 a 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 seller bank server; after receiving the has-been-received notification sent by the seller 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.

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2017 年 1 月 26 日 (26.01.2017)

WIPO | PCT

(10) 国际公布号
WO 2017/012063 A1

(51) 国际专利分类号:
G06Q 20/12 (2012.01) *G06Q 30/06* (2012.01)

(21) 国际申请号: PCT/CN2015/084660

(22) 国际申请日: 2015 年 7 月 21 日 (21.07.2015)

(25) 申请语言: 中文

(26) 公布语言: 中文

(71) 申请人: **深圳市银信网银科技有限公司 (SHENZHEN CIFPAY NETWORK BANK TECHNOLOGY CO., LTD)** [CN/CN]; 中国广东省深圳市福田区滨河路北彩田路东交汇处联合广场 A 座裙楼 402-D、402-E, Guangdong 518000 (CN)。

(72) 发明人: **张毅 (ZHANG, Yi)**; 中国广东省深圳市福田区滨河路北彩田路东交汇处联合广场 A 座裙楼 402-D、402-E, Guangdong 518000 (CN)。

(74) 代理人: **广东广和律师事务所 (GUANGDONG GUANGHE LAW FIRM)**; 中国广东省深圳市福田区福虹路世贸广场 A 座 20 层, Guangdong 518000 (CN)。

(81) 指定国 (除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明，要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

(54) Title: ONLINE TRANSACTION METHOD, DEVICE AND SYSTEM

(54) 发明名称 : 网上交易方法、装置和系统

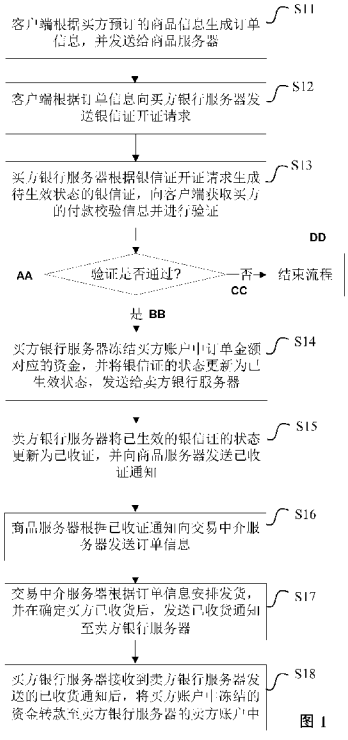


图 1

S11 CLIENT GENERATES ORDER INFORMATION ACCORDING TO INFORMATION OF ITEM ORDERED BY BUYER, AND SENDS ORDER INFORMATION TO ITEM SERVER
S12 CLIENT SENDS BANK CREDIT CERTIFICATE ISSUING REQUEST TO BUYER BANK SERVER ACCORDING TO ORDER INFORMATION
S13 BUYER BANK SERVER GENERATES BANK CREDIT CERTIFICATE HAVING TO-BE-EFFECTIVE STATUS ACCORDING TO BANK CREDIT CERTIFICATE ISSUING REQUEST, AND VERIFIES BUYER PAYMENT CHECKING INFORMATION OBTAINED BY CLIENT
S14 BUYER BANK SERVER FREEZES FUNDS IN BUYER ACCOUNT WHICH CORRESPOND TO ORDER AMOUNT, UPDATES STATUS OF BANK CREDIT CERTIFICATE TO EFFECTIVE STATUS, AND SENDS BANK CREDIT CERTIFICATE TO SELLER BANK SERVER
S15 SELLER BANK SERVER UPDATES STATUS OF EFFECTIVE BANK CREDIT CERTIFICATE TO HAS-BEEN-RECEIVED, AND SENDS HAS-BEEN-RECEIVED NOTIFICATION TO ITEM SERVER
S16 ITEM SERVER SENDS ORDER INFORMATION TO TRANSACTION INTERMEDIARY SERVER ACCORDING TO HAS-BEEN-RECEIVED NOTIFICATION
S17 TRANSACTION INTERMEDIARY SERVER ARRANGES DISPATCHING ACCORDING TO ORDER INFORMATION, AND AFTER DETERMINING THAT BUYER HAS RECEIVED, SENDS HAS-BEEN-RECEIVED NOTIFICATION TO SELLER BANK SERVER
S18 AFTER RECEIVING HAS-BEEN-RECEIVED NOTIFICATION SENT BY SELLER BANK SERVER, BUYER BANK SERVER TRANSFERS FROZEN FUNDS IN BUYER ACCOUNT INTO SELLER ACCOUNT OF SELLER BANK SERVER
AA IS VERIFICATION PASSED?
BB YES
CC NO
DD END PROCESS

(57) Abstract: Disclosed are an online transaction method, device and system, the method comprising the steps of: a client generates order information according to an item ordered by a buyer, and sends the order information to an item server; the client sends a bank credit certificate issuing request to a buyer bank server; the buyer bank server generates a bank credit certificate having a to-be-effective status, 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 a 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 seller bank server; after receiving the has-been-received notification sent by the seller 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.

(57) 摘要:

[见续页]

WO 2017/012063 A1

WO 2017/012063 A1

本发明公开了一种网上交易方法、装置和系统，所述方法包括步骤：客户端根据买方预订的商品生成订单信息，并发送给商品服务器；并向买方银行服务器发送银信证开证请求；买方银行服务器生成待生效状态的银信证，冻结买方账户中订单金额对应的资金，并将银信证的状态更新为已生效状态，并发送给卖方银行服务器；卖方银行服务器向商品服务器发送已收证通知；商品服务器向交易中介服务器发送订单信息；交易中介服务器根据安排发货，并向卖方银行服务器发送已收货通知；买方银行服务器接收到卖方银行服务器发送的已收货通知后，将买方账户中冻结的资金转款至卖方银行服务器的卖方账户中。从而降低了资金风险和提高了交易信息安全性。

Title: 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 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 fund risk and improving 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] The client generates order information according to the commodity ordered by the buyer, and delivers the order information to the commodity server; and delivers a Bank Credit Certificate issuing request to the buyer's bank server according to the order information;

[0009] The buyer bank server generates a bank credit certificate of the to-be-validated status according to the bank credit certificate issuing request, and acquires the buyer's payment verification information from the client and performs verification; when the verification passes, freeze the funds corresponding to the amount of the order in the account of the buyer's account, and updates the status of the Bank Credit Certificate to a valid status and delivers the status to the seller's bank server;

[0010] 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;

[0011] The commodity server delivers the order information to the transaction intermediation server according to the received card notification;

[0012] 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;

[0013] The seller bank server delivers the receipt notification to the buyer bank server;

[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] Receiving the order information delivered by the client;

[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, which is applied to an intermediation transaction server, the method including the steps of:

[0019] After receiving the order information delivered by the commodity server, and arrange the delivery according to the order information;

[0020] After determining that the buyer has received the commodity, deliver the commodity receipt notification to the seller bank 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 issuance request delivered by the client, a Bank Credit Certificate of the status to be validated is generated;

[0023] Obtain the buyer's payment check information to the client and verify;

[0024] 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;

[0025] After receiving the received notification delivered by the seller's bank server, the funds frozen by the buyer's account are transferred to the seller's account of the seller's bank server.

[0026] According to another aspect of the present invention, it is provided an online transaction system including a client, a commodity server, a buyer bank server, a seller bank server, and a transaction intermediation server, wherein:

[0027] The client is used to generate order information according to the commodity ordered by the buyer and deliver the order information to the commodity server; and deliver a Bank Credit Certificate issuing request to the buyer's bank server according to the order information;

[0028] The commodity server is used to receive the order information delivered by the client; after receiving the received certificate notification delivered by the seller bank server, deliver the order information to the transaction intermediation server;

[0029] The seller bank server is used to, after receiving the valid Bank Credit Certificate delivered by the buyer bank server, update the status of the Bank Credit Certificate to a certified status, and deliver the notification to the commodity server; and after receiving the receipt notification delivered by the transaction intermediation server, delivering the receipt notification to the buyer bank server;

[0030] 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;

[0031] The buyer bank server is used to generate a Bank Credit Certificate to be validated according to a Bank Credit Certificate issuing request delivered by the client, acquire buyer's payment verification information from the client, and perform 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.

[0032] According to another aspect of the present invention, it is provided an online transaction device applied to a commodity server, including the following modules:

[0033] 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;

[0034] 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.

[0035] According to another aspect of the present invention, it is provided an online transaction device, which is applied to an intermediation transaction server and includes the following modules:

[0036] A fourth receiving module is used to receive the order information delivered by the commodity server;

[0037] Delivery scheduling module is set up to arrange delivery according to the information of the order;

[0038] The first received notification module is used to deliver a receipt notification to the seller's bank server after determining that the buyer has received the commodity.

[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] The third receiving module is used to receive the Bank Credit Certificate issuing request delivered by the client and the received notification delivered by the seller bank server;

[0041] 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;

[0042] A verification module is used to obtain the buyer's payment verification information and to verify to the client;

[0043] 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;

[0044] 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.

[0045] The online trading method, device and system provided by the present invention, deliver the issuing request to the buyer's bank server through the Client, the seller bank server 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

[0046] 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 technology to communicate, to further improve the security of the transaction.

Brief Description of the Drawings

[0047] Figure 1 is a flowchart of a first example of the online transaction method of the present invention;

[0048] Figures 2A and 2B are an interactive diagram of each system in a transaction process in an example of the present invention;

[0049] 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

Date Reçue/Date Received 2020-07-14

of the present invention;

[0050] Figure 4 is a flowchart of a second example of the online transaction method of the present invention;

[0051] Figure 5 is a flowchart of the third example of the online transaction method of the present invention;

[0052] Figure 6 is a flowchart of a fourth example of the online transaction method of the present invention;

[0053] Figure 7 is a flow chart of the fifth example of the online transaction method of the present invention;

[0054] Figure 8 is a block diagram of the first example of the online trading system of the present invention;

[0055] Figure 9 is a schematic block diagram of an example of an online transaction device applied to a client according to the present invention;

[0056] 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;

[0057] 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;

[0058] 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;

[0059] 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;

[0060] Figure 14 is a schematic block diagram of a second example of the online trading system of the present invention.

Detailed Description

[0061] 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.

[0062] It is to be understood that the specific examples described herein are merely illustrative of the invention but not intended to limit the invention.

[0063] Please refer to Figure 1 and Figures 2A and 2B, an example of the online transaction

Date Reçue/Date Received 2020-07-14

method of the present invention is proposed, and the method includes the following steps:

[0064] S11: the client generates order information according to the commodity information ordered by the buyer and delivers it to the commodity server.

[0065] 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.

[0066] 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

Date Reçue/Date Received 2020-07-14

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.

[0067] S12: the client delivers a Bank Credit Certificate issuing request to the buyer's bank server according to the order information.

[0068] 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).

[0069] In step S12, the client obtains 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 buyer bank server. Wherein, Bank 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.

[0070] S13: the buyer bank server generates a Bank Credit Certificate to be validated according to a Bank Credit Certificate issuing request, acquires the buyer's payment verification information from the client, and performs verification. If the verification succeeds, step S14 is performed, otherwise, the process ends.

[0071] In this step S13, after receiving the Bank Credit Certificate issuing request, obtains the seller bank server, generates a 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.

[0072] Specifically, after generating the Bank Credit Certificate Z1 in the to-be-validated state, 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.

[0073] S14: 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.

[0074] 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 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.

[0075] 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.

[0076] In step S15, 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 already been validated, and delivers the received card notification to the commodity server.

[0077] S16: the commodity server delivers the order information to the transaction intermediation server according to the received card notification.

[0078] In this step S17, after receiving the commodity receipt notification, the commodity server delivers the order information to the transaction intermediation server.

[0079] 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.

[0080] 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.

[0081] 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.

[0082] S18: After receiving the receipt notification delivered by the seller's bank server, the buyer bank server transfers the funds frozen in the buyer's account to the seller's account of the seller's bank server.

[0083] In this step S18, after receiving the receipt notification delivered by the transaction intermediation server, the seller bank server delivers the receipt notification to the buyer bank server, and the buyer's bank server transfers the funds frozen in the buyer's account to the seller's account according to the notification receipt. At this point, the transaction is completed.

[0084] 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.

[0085] 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.

[0086] 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.

[0087] 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:

[0088] S101: the data deliverer generates a symmetric key, and encrypts the communication data by using a symmetric key to form a first ciphertext.

[0089] 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 the symmetric key to form the first ciphertext.

[0090] S102: the data deliverer encrypts the symmetric key by using the public key of the data receiver to form a second ciphertext.

[0091] 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.

[0092] 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.

[0093] S105: After the verification is passed, the data receiver decrypts the second ciphertext using its private key to obtain a symmetric key.

[0094] S106: The data receiver uses the symmetric key to decrypt the first ciphertext to obtain the communication data

[0095] In some examples, the signature step in step S103 and the verification signature step in step S104 may also be omitted.

[0096] 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.

[0097] 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.

[0098] 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:

[0099] S21, receiving the order information delivered by the client.

[0100] S22, after receiving the received card notification delivered by the seller's bank server, deliver the order information to the transaction intermediation server.

[0101] 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.

[0102] 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:

[0103] S31, 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.

[0104] S32, after receiving the receipt notification delivered by the transaction intermediation server, delivering the receipt notification to the buyer bank server.

[0105] 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:

[0106] S41, after receiving the Bank Credit Certificate issuance request delivered by the client, a Bank Credit Certificate of the valid status is generated, and the buyer's payment verification information is obtained from the client and verified. If the verification is passed, step S602 is executed, otherwise, the flow is ended.

[0107] 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.

[0108] S43. After receiving the receipt notification delivered by the seller's bank server, the funds frozen by the buyer's account are transferred to the seller's account of the seller's bank server.

[0109] 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:

[0110] S51, receiving the order information delivered by the commodity server, and arranging the delivery according to the order information.

[0111] 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.

[0112] S52, After determining that the buyer has received the commodity, deliver the commodity receipt notification to the seller bank server

[0113] 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.

[0114] 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:

[0115] The client terminal is used to obtain commodity information from the commodity server, generate an order according to the commodity ordered by the buyer, and deliver the order to a commodity server; and deliver a Bank Credit Certificate issuing request to the buyer's bank server according to the order information; 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.

[0116] Wherein, please refer to Figure 9, an online transaction device applied to a client includes the following modules:

[0117] 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;

[0118] Opening certificate requesting module is used to deliver a bank credit certificate issuing request to the first bank server according to the generated order information;

[0119] 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.

[0120] The commodity server is used to receive the order information delivered by the client, and after receiving the received certificate notification delivered by the seller bank server, deliver the order information to the transaction intermediation server.

[0121] Please refer to Figure 10, an online trading device applied to a commodity server includes the following modules:

[0122] 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;

[0123] 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.

[0124] The seller bank server is used to, after receiving the valid Bank Credit Certificate delivered by the buyer bank server, update the status of the Bank Credit Certificate to a certified status, and deliver the notification to the commodity server; and after receiving the receipt notification delivered by the transaction intermediation server, delivering the receipt notification to the buyer bank server.

[0125] Wherein, refer to Figure 11, the online trading device applied to the seller's bank server includes the following modules:

[0126] A second 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;

[0127] 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.

[0128] The second receipt notification module is used to deliver a receipt notification of receipt to the buyer's bank server after receiving the receipt notification delivered by the transaction intermediation server.

[0129] The buyer bank server: set to receive Bank Credit Certificate delivered by the client request, generate Bank Credit Certificate 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 seller 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.

[0130] Wherein, please refer to Figure 12, the online trading device applied to the buyer's bank server includes the following modules:

[0131] The third receiving module is used to receive the Bank Credit Certificate issuing request delivered by the client and the received notification delivered by the seller bank server;

[0132] Bank Credit Certificate generating module is used for generating a Bank Credit Certificate to be validated according to a Bank Credit Certificate issuing request;

[0133] A verification module is used to acquire the buyer's payment verification information from the client according to the Bank Credit Certificate to be validated, and verify the payment verification information;

[0134] 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;

[0135] The money transfer module is used to after receiving the receipt notification delivered by the seller's bank server, the funds frozen by the buyer's account are transferred to the seller's account of the seller's bank server.

[0136] 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 seller bank 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.

[0137] 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.

[0138] Wherein, please refer to Figure 13, an online transaction device applied to a transaction intermediation server includes the following modules:

[0139] A fourth receiving module is used to receive the order information delivered by the commodity server;

[0140] 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;

[0141] The first received notification module is used to deliver a receipt notification to the seller's bank server after determining that the buyer has received the commodity. Specifically, after the receiving notification module receives the first receiving confirmation notification delivered by the client, it determines that the buyer has received the commodity; or, the first 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.

[0142] 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 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.

[0143] 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.

[0144] 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.

[0145] 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:

[0146] 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.

[0147] 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 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.

[0148] 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:

[0149] 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.

[0150] 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.

[0151] 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:

[0152] 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.

[0153] 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.

[0154] 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.

[0155] 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

[0156] 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.

[0157] 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

[0158] According to the method, device and system for online transaction method of the present invention, a client delivers an issuing request to a buyer's bank server through a client, the seller bank server delivers a receipt notification to the buyer's bank server, and delivers the receipt notification to 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

Date Reçue/Date Received 2020-06-23

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 2020-06-23

Claims:

1. A computer system for online transaction, the system comprising:

a buyer's device configured to:

generate and deliver order information according to an order of commodity by a buyer to a commodity server; and

deliver a request for issuing a Bank Credit Certificate to a buyer's bank server according to the order information to achieve a transaction process within a banking system rather than a third-party payment platform for supervising funds and reducing risks of funds;

the buyer's bank server configured to:

generate a to-be-validated Bank Credit Certificate according to a request for issuing the Bank Credit Certificate for monitoring transaction status in real time by generating Bank Credit Certificate so as to keep time of fund flow in sync with actual transaction time;

acquire buyer's payment verification information from the buyer's device to perform a verification process;

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

Date reçue / Date received 2021-11-05

validate the to-be-validated Bank Credit Certificate for delivering the validated Bank Credit Certificate to a seller's bank server; wherein the Bank Credit Certificate is an electronic commitment payment certificate issued by the buyer's bank sever for transferring encrypted transaction data between the buyer's bank and the seller's bank;
and

unfreeze the 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 via the seller's bank server;

the seller's bank server configured to:

update the validated the Bank Credit Certificate to a received status when receiving the validated Bank Credit Certificate;

deliver a notification for receiving the Bank Credit Certificate to the commodity server; and

deliver a receipt notification for commodity delivery to the buyer's bank server according to the validated Bank Credit Certificate for transferring the amount of funds to the seller's account when receiving the receipt notification for commodity delivery from a transaction intermediation server;

the commodity server configured to:

receive the order information delivered by the buyer's device; and

Date reçue / Date received 2021-11-05

deliver the order information to a transaction intermediation server when receiving the notification for receiving the Bank Credit Certificate delivered by the seller's bank server; and

the transaction intermediation server configured to arrange a shipment for the commodity according to the order information and deliver the receipt notification for commodity delivery to the seller's bank server after determining that the buyer has received the commodity; and

wherein the order information, the request, the notification, the receipt notification and information of shipment are communicative data encrypted via digital envelopes to ensure security of data transactions.

2. The system of claim 1, wherein the Bank Credit Certificate may be stored in a computer system and transmitted between the buyer's bank server and the seller's bank server via the Internet.

3. The system of claim 1, wherein the buyer's device is configured to transmit communicative data to the buyer's bank server and the commodity server respectively via digital envelopes for data security.

4. The system of claim 1, wherein the buyer's bank server is configured to transmit communicative data to the buyer's device and the seller's bank server respectively via digital envelopes for data security.

5. The system of claim 1, wherein the seller's bank server is configured to transmit communicative data to the transaction intermediation server and the buyer's bank server respectively via digital envelopes for data security.

Date reçue / Date received 2021-11-05

6. The system of claim 1, wherein the commodity server is configured to transmit communicative data to the transaction intermediation server, the seller's bank server and the buyer's device respectively via digital envelopes for data security.

7. The system of claim 1, wherein the transaction intermediation server is configured to transmit communicative data to the commodity server and the seller's bank server respectively via digital envelopes for data security.

8. The system of any one of claims 1 to 7, wherein transmitting communicative data via digital envelopes for data security further includes a data sender.

9. The system of claim 8, wherein the data sender is configured to:

generate 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 a data receiver to encrypt the symmetric key to form a second ciphertext; and

deliver the first ciphertext and the second ciphertext to a data receiver.

10. The system of any one of claims 1 to 9, wherein transmitting communicative data via digital envelopes for data security further includes a data receiver.

11. The system of any one of claims 9 to 10, wherein the data receiver is configured to:

decrypt the second ciphertext by using an owned private key to obtain the symmetric key; and

decrypt the first ciphertext by using the symmetric key to obtain the communicative data.

Date reçue / Date received 2021-11-05

12. The system of any one of claims 9 to 11, wherein the data deliverer is further configured to sign digitally the first ciphertext and the second ciphertext respectively by using the own private key.

13. The system of any one of claims 9 to 12, wherein the data receiver is further configured to verify the first ciphertext and the second ciphertext with the digital signs respectively by using the public key from the data deliverer.

14. The system of any one of claims 9 to 13, wherein the data sender is further configured to randomly generate the symmetric key dynamically.

15. The system of any one of claims 9 to 14, wherein the data sender is further configured to encrypt the communicative data by using the symmetric key based on Advanced Encryption Standard (AES) algorithm to form the first ciphertext.

16. The system of any one of claims 8 to 14 further includes a monitoring server.

17. The system of claim 16, wherein the monitoring server is further configured to simultaneously collect the data delivered by the data deliverer and the data received by the data receiver to verify the consistency of the transmitted data and the received data in a data transmission process.

18. The system of any one of claims 1 to 17, wherein the buyer's device may be the data sender when sending the communicative data.

19. The system of any one of claims 1 to 17, wherein the commodity server may be the data sender when sending the communicative data.

20. The system of any one of claims 1 to 17, wherein the buyer's bank server may be the data sender when sending the communicative data.

Date reçue / Date received 2021-11-05

21. The system of any one of claims 1 to 17, wherein the seller's bank server may be the data sender when sending the communicative data.

22. The system of any one of claims 1 to 17, wherein the transaction intermediation server may be the data sender when sending the communicative data.

23. The system of any one of claims 1 to 22, wherein the buyer's device may be the data receiver when receiving the communicative data.

24. The system of any one of claims 1 to 22, wherein the commodity server may be the data receiver when receiving the communicative data.

25. The system of any one of claims 1 to 22, wherein the buyer's bank server may be the data receiver when receiving the communicative data.

26. The system of any one of claims 1 to 22, wherein the seller's bank server may be the data receiver when receiving the communicative data.

27. The system of any one of claims 1 to 22, wherein the transaction intermediation server may be the data sender when receiving the communicative data.

28. The system of any one of claims 1 to 27, wherein the communicative data is transmitted among the buyer's device, the commodity server, the buyer's bank server and the seller's bank server through a public network.

29. The system of any one of claims 1 to 27, wherein the communicative data is transmitted between the monitoring server and the buyer's bank server and the seller's bank server respectively via dedicated line communication.

Date reçue / Date received 2021-11-05

30. The system of any one of claims 1 to 29, wherein the transaction intermediation server is configured to determine that the buyer has received the commodity after receiving a receipt confirmation notification for the commodity delivery delivered by the buyer's device.

31. The system of any one of claims 1 to 30, wherein the transaction intermediation server is configured to determine that the buyer has received the commodity beyond the pre-set delivery period, when the transaction intermediation server fails to receive the receipt confirmation notification for the commodity delivery from the buyer's device within a pre-set delivery period.

32. The system of any one of claims 1 to 31, wherein the buyer's bank server may be a computer server corresponding to the buyer's bank account.

33. The system of any one of claims 1 to 31, wherein the seller's bank server may be a computer server corresponding to the seller's bank account.

34. The system of any one of claims 1 to 33, wherein the seller's bank server may be the same with the buyer's bank server.

35. The system of any one of claims 1 to 33, wherein the seller's bank server may be different from the buyer's bank server.

36. The system of any one of claims 1 to 35, wherein the payment verification information may be a webpage for payment.

37. The system of claim 36, wherein the webpage for payment is configured to be inputted verification information by the buyer via the buyer's device.

38. The system of any one of claims 36 to 37, wherein the verification information includes buyer's bank account number.

Date reçue / Date received 2021-11-05

39. The system of any one of claims 36 to 38, wherein the verification information includes password of the buyer's bank account.

40. The system of any one of claims 36 to 39, wherein the verification information includes verification code.

41. The system of any one of claims 36 to 40, wherein the verification information includes expiration date.

42. The system of any one of claims 36 to 41, wherein the webpage for payment is configured to be inputted payment amount by the buyer via the buyer's device.

43. A computer implemented method for online transaction, the method comprising:

a buyer's device generates and delivers order information according to an order of commodity by a buyer to a commodity server; and

the buyer's bank server generates a to-be-validated Bank Credit Certificate according to a request for issuing a Bank Credit Certificate for monitoring transaction status in real time by generating Bank Credit Certificate so as to keep time of fund flow in sync with actual transaction time, when receiving the request for issuing the Bank Credit Certificate from the buyer's device according to the order information to achieve a transaction process within a banking system rather than a third-party payment platform for supervising funds and reducing risks of funds;

the buyer's bank server acquires buyer's payment verification information from the buyer's device to perform a verification process;

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

Date reçue / Date received 2021-11-05

the buyer's bank server validates the Bank Credit Certificate for delivering the validated Bank Credit Certificate to a seller's bank server; wherein the Bank Credit Certificate is an electronic commitment payment certificate issued by the buyer's bank sever for transferring encrypted transaction data between the buyer's bank and the seller's bank

the seller's bank server delivers a notification for receiving the Bank Credit Certificate to the commodity server after updating the validated the Bank Credit Certificate to a received status when receiving the validated Bank Credit Certificate;

the commodity server delivers the order information to a transaction intermediation server when receiving the notification for receiving the Bank Credit Certificate delivered by the seller's bank server;

the transaction intermediation server arranges a shipment for the commodity according to the order information and delivers a receipt notification for commodity delivery to the seller's bank server after determining that the buyer has received the commodity;

the seller's bank server delivers the receipt notification for commodity delivery to the buyer's bank server according to the validated Bank Credit Certificate for transferring the amount of funds to the seller's account when receiving the receipt notification for commodity delivery from the transaction intermediation server; and

the buyer bank server unfreezes the 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 the receipt notification for commodity delivery via the seller's bank server; and

wherein the order information, the request, the notification, the receipt notification and information of shipment are communicative data encrypted via digital envelopes to ensure security of data transactions.

Date reçue / Date received 2021-11-05

44. The method of claim 43, wherein the Bank Credit Certificate may be stored in a computer system and transmitted between the buyer's bank server and the seller's bank server via the Internet.

45. The method of claim 43 further includes that the buyer's device transmits communicative data to the buyer's bank server and the commodity server respectively via digital envelopes for data security.

46. The method of claim 43 further includes that the buyer's bank server transmits communicative data to the buyer's device and the seller's bank server respectively via digital envelopes for data security.

47. The method of claim 43 further includes that the seller's bank server transmits communicative data to the transaction intermediation server and the buyer's bank server respectively via digital envelopes for data security.

48. The method of claim 43 further includes that the commodity server transmits communicative data to the transaction intermediation server, the seller's bank server and the buyer's device respectively via digital envelopes for data security.

49. The method of claim 43 further includes that the transaction intermediation server transmits communicative data to the commodity server and the seller's bank server respectively via digital envelopes for data security.

50. The method of any one of claims 43 to 49, wherein transmitting communicative data via digital envelopes for data security further includes that

Date reçue / Date received 2021-11-05

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 owned private key to obtain the symmetric key and decrypts the first ciphertext by using the symmetric key to obtain the communicative data.

51. The method of claim 50 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.

52. The method of claim 50, wherein the data sender randomly generates the symmetric key dynamically.

53. The method of claim 50, wherein the data sender encrypts the communicative data by using the symmetric key based on Advanced Encryption Standard (AES) algorithm to form the first ciphertext.

54. The method of any one of claims 43 to 53 further includes a monitoring server simultaneously collects the data delivered by the data deliverer and the data received by the data receiver to verify the consistency of the transmitted data and the received data in a data transmission process.

55. The method of any one of claims 43 to 54, wherein the buyer's device may be the data sender when sending the communicative data.

Date reçue / Date received 2021-11-05

56. The method of any one of claims 43 to 54, wherein the commodity server may be the data sender when sending the communicative data.

57. The method of any one of claims 43 to 54, wherein the buyer's bank server may be the data sender when sending the communicative data.

58. The method of any one of claims 43 to 54, wherein the seller's bank server may be the data sender when sending the communicative data.

59. The method of any one of claims 43 to 54, wherein the transaction intermediation server may be the data sender when sending the communicative data.

60. The method of any one of claims 43 to 59, wherein the buyer's device may be the data receiver when receiving the communicative data.

61. The method of any one of claims 43 to 59, wherein the commodity server may be the data sender when receiving the communicative data.

62. The method of any one of claims 43 to 59, wherein the buyer's bank server may be the data sender when receiving the communicative data.

63. The method of any one of claims 43 to 59, wherein the seller's bank server may be the data sender when receiving the communicative data.

64. The method of any one of claims 43 to 59, wherein the transaction intermediation server may be the data sender when receiving the communicative data.

65. The method of any one of claims 43 to 64, wherein the communicative data is transmitted among the buyer's device, the commodity server, the buyer's bank server and the seller's bank server through a public network.

Date reçue / Date received 2021-11-05

66. The method of any one of claims 43 to 65, wherein the communicative data is transmitted between the monitoring server and the buyer's bank server and the seller's bank server respectively via dedicated line communication.

67. The method of any one of claims 43 to 66 further includes that

the transaction intermediation server determines that the buyer has received the commodity after receiving a receipt confirmation notification for the commodity delivery delivered by the buyer's device; and

the transaction intermediation server determines that the buyer has received the commodity beyond the pre-set delivery period, when the transaction intermediation server fails to receive the receipt confirmation notification for the commodity delivery from the buyer's device within a pre-set delivery period.

68. The method of any one of claims 43 to 67, wherein the buyer's bank server may be a computer server corresponding to the buyer's bank account.

69. The method of any one of claims 43 to 67, wherein the seller's bank server may be a computer server corresponding to the seller's bank account.

70. The method of any one of claims 43 to 69, wherein the seller's bank server may be the same with the buyer's bank server.

71. The method of any one of claims 43 to 69, wherein the seller's bank server may be different from the buyer's bank server.

72. The method of any one of claims 43 to 71, wherein the payment verification information may be a webpage for payment.

Date reçue / Date received 2021-11-05

73. The method of claim 72, wherein the webpage for payment is configured to be inputted verification information by the buyer via the buyer's device.

74. The method of any one of claims 72 to 73, wherein the verification information includes buyer's bank account number.

75. The method of any one of claims 72 to 74, wherein the verification information includes password of the buyer's bank account.

76. The method of any one of claims 72 to 75, wherein the verification information includes verification code.

77. The method of any one of claims 72 to 76, wherein the verification information includes expiration date.

78. The method of any one of claims 72 to 77, wherein the webpage for payment is configured to be inputted payment amount by the buyer via the buyer's device.

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

generating a to-be-validated Bank Credit Certificate according to a request for issuing a Bank Credit Certificate when receiving a request for issuing the Bank Credit Certificate delivered by a buyer's device;

acquiring buyer's payment verification information from the buyer's 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 of commodity when the verification process is passed;

Date reçue / Date received 2021-11-05

validating the to-be-validated Bank Credit Certificate for delivering the validated Bank Credit Certificate to a seller's bank server; wherein the Bank Credit Certificate is an electronic commitment payment certificate issued by a bank sever for transferring encrypted data between the buyer's bank and the seller's bank; and

unfreezing the frozen amount of funds in a buyer's account to transfer the amount of funds to a seller's account through a seller's bank server, after receiving a receipt notification for commodity delivery via the seller's bank server; and

wherein the request, the receipt notification are communicative data encrypted via digital envelopes to ensure security of data transactions.

80. The method of claim 79, wherein the Bank Credit Certificate may be stored in a computer system and transmitted between the buyer's bank server and the seller's bank server via the Internet.

81. The method of claim 79 further includes transmitting communicative data to the buyer's device and the seller's bank server respectively via digital envelopes for data security.

82. The method of claim 80, 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 owned private key to obtain the symmetric key and decrypts the first ciphertext by using the symmetric key to obtain the communicative data.

Date reçue / Date received 2021-11-05

83. The method of claim 82 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.

84. The method of claim 82, wherein the data sender randomly generates the symmetric key dynamically.

85. The method of claim 82, wherein the data sender encrypts the communicative data by using the symmetric key based on Advanced Encryption Standard (AES) algorithm to form the first ciphertext.

86. The method of any one of claims 79 to 85, wherein the buyer's device may be the data sender when sending the communicative data.

87. The method of any one of claims 79 to 85, wherein the buyer's bank server may be the data sender when sending the communicative data.

88. The method of any one of claims 79 to 85, wherein the buyer's bank server may be the data receiver when receiving the communicative data.

89. The method of any one of claims 79 to 85, wherein the seller's bank server may be the data sender when sending the communicative data.

90. The method of any one of claims 79 to 85, wherein the seller's bank server may be the data receiver when receiving the communicative data.

Date reçue / Date received 2021-11-05

91. The method of any one of claims 80 to 90, wherein the communicative data is transmitted among the buyer's device, a commodity server, the buyer's bank server and the seller's bank server through a public network.

92. The method of any one of claims 80 to 91, wherein the communicative data is transmitted between a monitoring server and the buyer's bank server and the seller's bank server respectively via dedicated line communication.

93. The method of any one of claims 79 to 92, wherein the buyer's bank server may be a computer server corresponding to the buyer's bank account.

94. The method of any one of claims 79 to 92, wherein the seller's bank server may be a computer server corresponding to the seller's bank account.

95. The method of any one of claims 79 to 94, wherein the seller's bank server may be the same with the buyer's bank server.

96. The method of any one of claims 79 to 94, wherein the seller's bank server may be different from the buyer's bank server.

97. The method of any one of claims 79 to 96, wherein the payment verification information may be a webpage for payment.

98. The method of claim 97, wherein the webpage for payment is configured to be inputted verification information by the buyer via the buyer's device.

99. The method of any one of claims 97 to 98, wherein the verification information includes buyer's bank account number.

100. The method of any one of claims 97 to 99, wherein the verification information includes password of the buyer's bank account.

Date reçue / Date received 2021-11-05

101. The method of any one of claims 97 to 100, wherein the verification information includes verification code.

102. The method of any one of claims 97 to 101, wherein the verification information includes expiration date.

103. The method of any one of claims 97 to 102, wherein the webpage for payment is configured to be inputted payment amount by the buyer via the buyer's device.

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

a third receiving module configured to:

receive a request for issuing a Bank Credit Certificate delivered by a buyer's device; and

receive a receipt notification for commodity delivery via the seller's bank server;

a Bank Credit Certificate generating module configured to generate a to-be-validated Bank Credit Certificate according to a request for issuing the Bank Credit Certificate;

a verification module configured to acquire buyer's payment verification information from the buyer's 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 of commodity when the verification process is passed; and

Date reçue / Date received 2021-11-05

validate the to-be-validated Bank Credit Certificate for delivering the validated Bank Credit Certificate to a seller's bank server; wherein the Bank Credit Certificate is an electronic commitment payment certificate issued by a bank sever for transferring encrypted data between the buyer's bank and the seller's bank;

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

wherein the request, the notification, the receipt notification are communicative data encrypted via digital envelopes to ensure security of data transaction.

105. The device of claim 104, wherein the Bank Credit Certificate may be stored in a computer system and transmitted between the buyer's bank server and the seller's bank server via the Internet.

106. The device of claim 104, wherein the third receiving module is further configured to transmit communicative data with the buyer's device and the seller's bank server respectively via digital envelopes for data security.

107. The device of claim 104, wherein the verification module is further configured to transmit communicative data with the buyer's device via digital envelopes for data security.

108. The device of claim 104, 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 2021-11-05

109.The device of claim 104, wherein the money transfer module is further configured to transmit communicative data with the seller's bank server via digital envelopes for data security.

110.The device of any one of claims 105 to 109, 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 owned private key to obtain the symmetric key and decrypts the first ciphertext by using the symmetric key to obtain the communicative data.

111.The device of claim 110 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.

112.The device of claim 110, wherein the data sender randomly generates the symmetric key dynamically.

113.The device of claim 110 wherein the data sender encrypts the communicative data by using the symmetric key based on Advanced Encryption Standard (AES) algorithm to form the first ciphertext.

Date reçue / Date received 2021-11-05

114.The device of any one of claims 104 to 113, wherein the buyer's device may be the data sender when sending the communicative data.

115.The device of any one of claims 104 to 113, wherein the buyer's bank server may be the data sender when sending the communicative data.

116.The device of any one of claims 104 to 113, wherein the buyer's bank server may be the data receiver when receiving the communicative data.

117.The device of any one of claims 104 to 113, wherein the seller's bank server may be the data sender when sending the communicative data.

118.The device of any one of claims 104 to 113, wherein the seller's bank server may be the data receiver when receiving the communicative data.

119.The device of any one of claims 105 to 113, wherein the communicative data is transmitted among the buyer's device, a commodity server, the buyer's bank server and the seller's bank server through a public network.

120.The device of any one of claims 105 to 113, wherein the communicative data is transmitted between a monitoring server and the buyer's bank server and the seller's bank server respectively via dedicated line communication.

121.The device of any one of claims 104 to 120, wherein the buyer's bank server may be a computer server corresponding to the buyer's bank account.

122.The device of any one of claims 104 to 121, wherein the seller's bank server may be a computer server corresponding to the seller's bank account.

123.The device of any one of claims 104 to 122, wherein the seller's bank server may be the same with the buyer's bank server.

Date reçue / Date received 2021-11-05

124.The device of any one of claims 104 to 122, wherein the seller's bank server may be different from the buyer's bank server.

125.The device of any one of claims 104 to 124, wherein the payment verification information may be a webpage for payment.

126.The device of claim 125, wherein the webpage for payment is configured to be inputted verification information by the buyer via the buyer's device.

127.The device of any one of claims 125 to 126, wherein the verification information includes buyer's bank account number.

128.The device of any one of claims 125 to 127, wherein the verification information includes password of the buyer's bank account.

129.The device of any one of claims 125 to 128, wherein the verification information includes verification code.

130.The device of any one of claims 125 to 129, wherein the verification information includes expiration date.

131. The device of any one of claims 125 to 130, wherein the webpage for payment is configured to be inputted payment amount by the buyer via the buyer's device.

Date reçue / Date received 2021-11-05

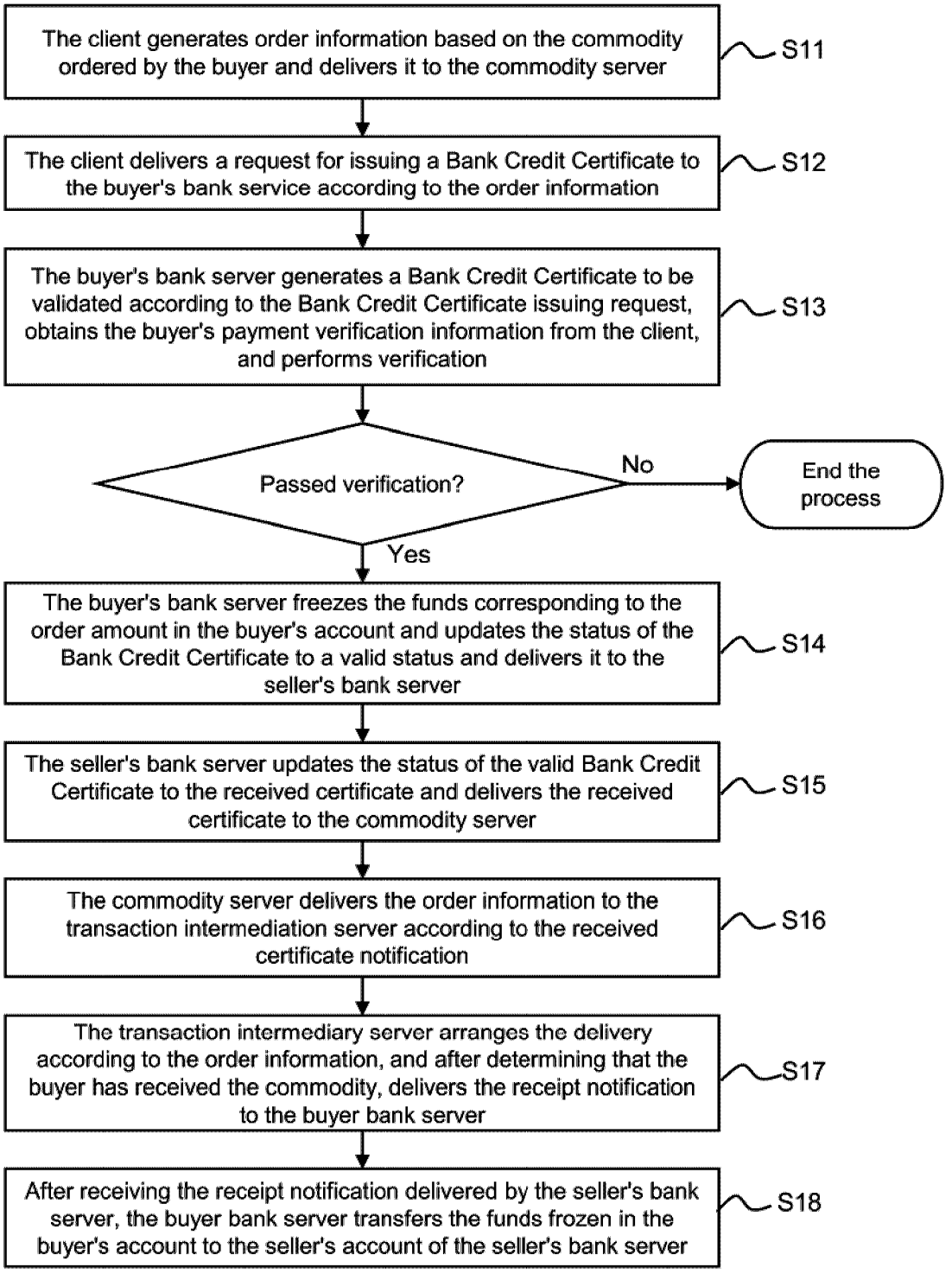


Figure 1

Date Reçue/Date Received 2020-07-14

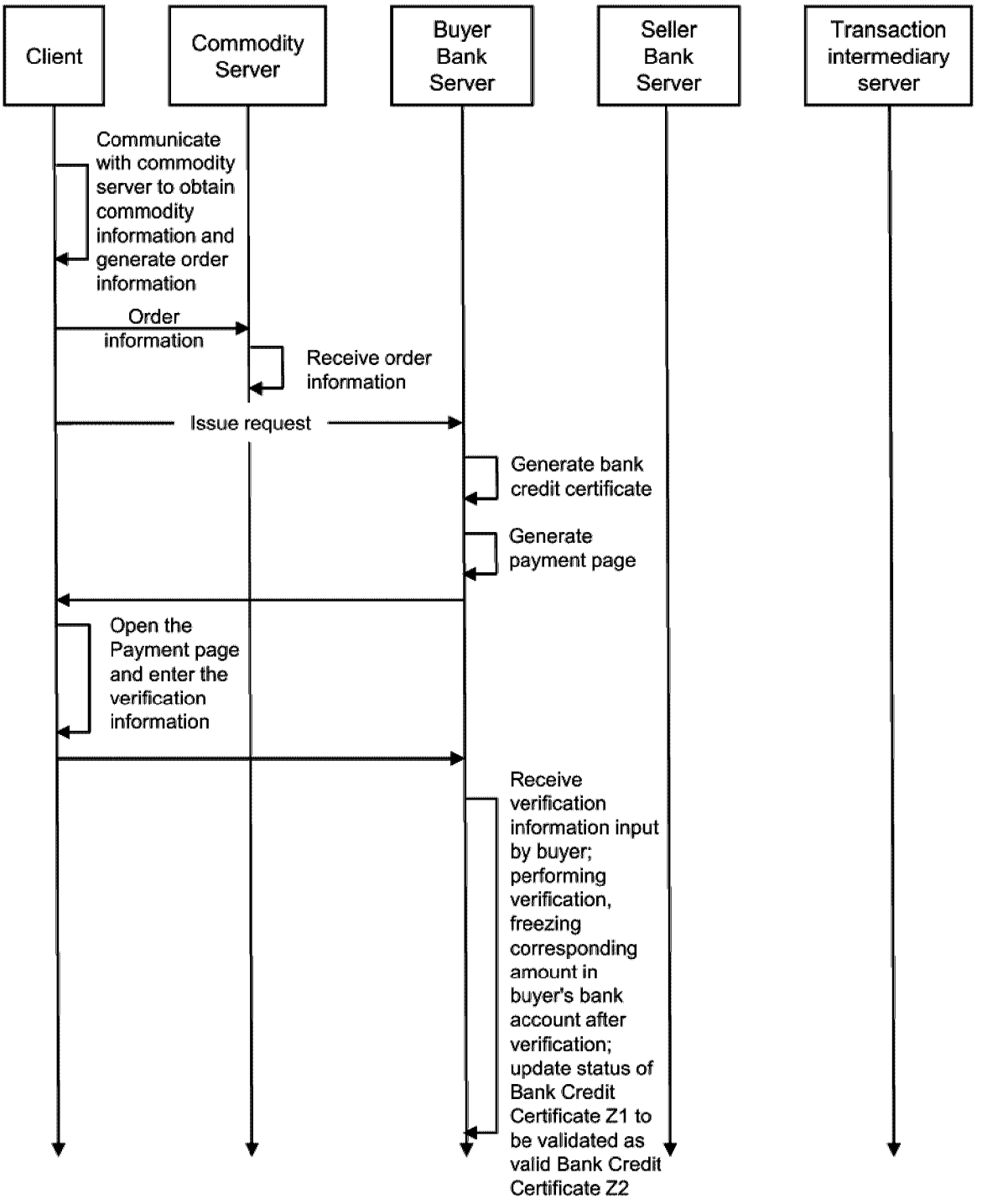


Figure 2A

Date Reçue/Date Received 2020-07-14

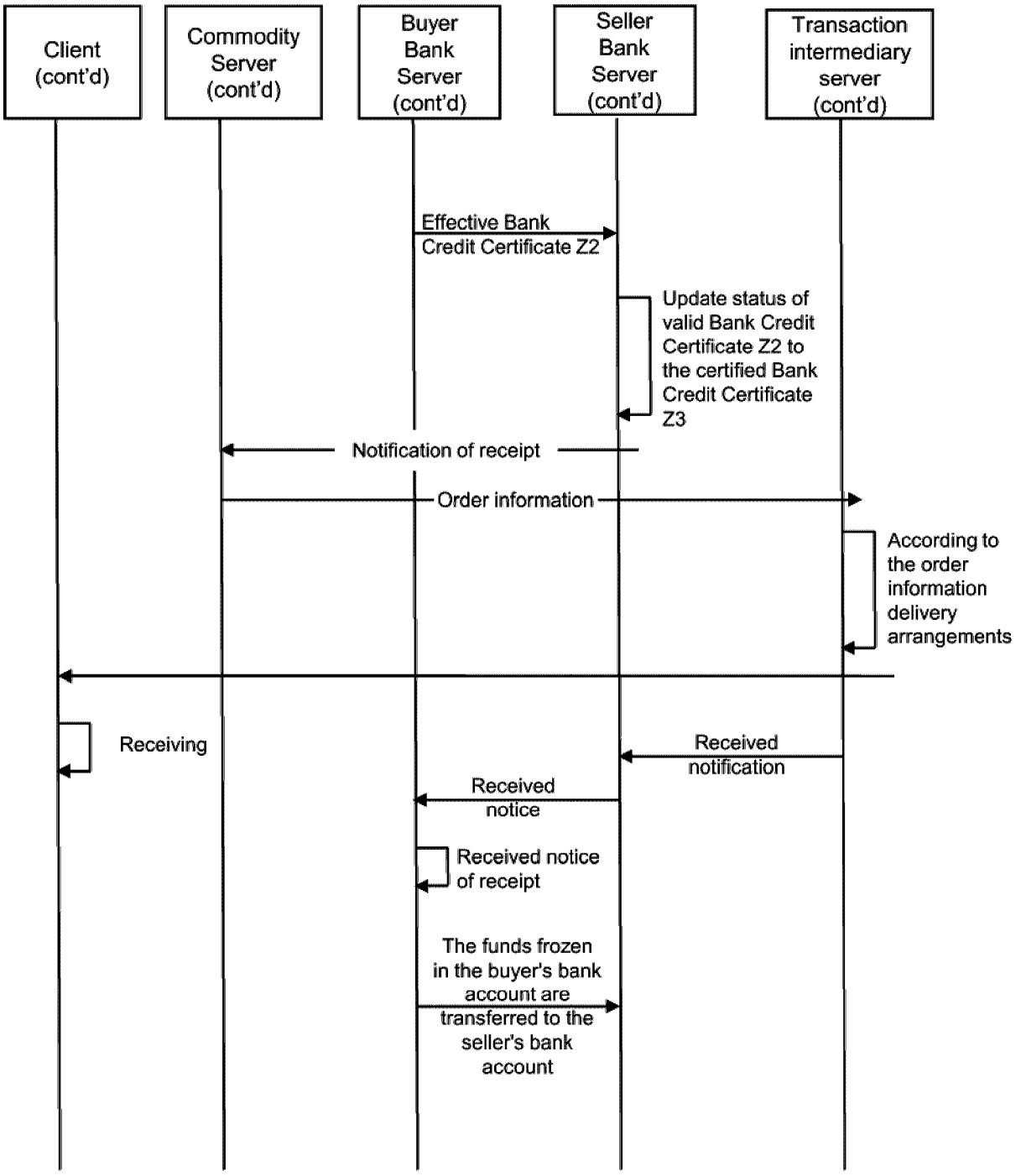


Figure 2B

Date Reçue/Date Received 2020-07-14

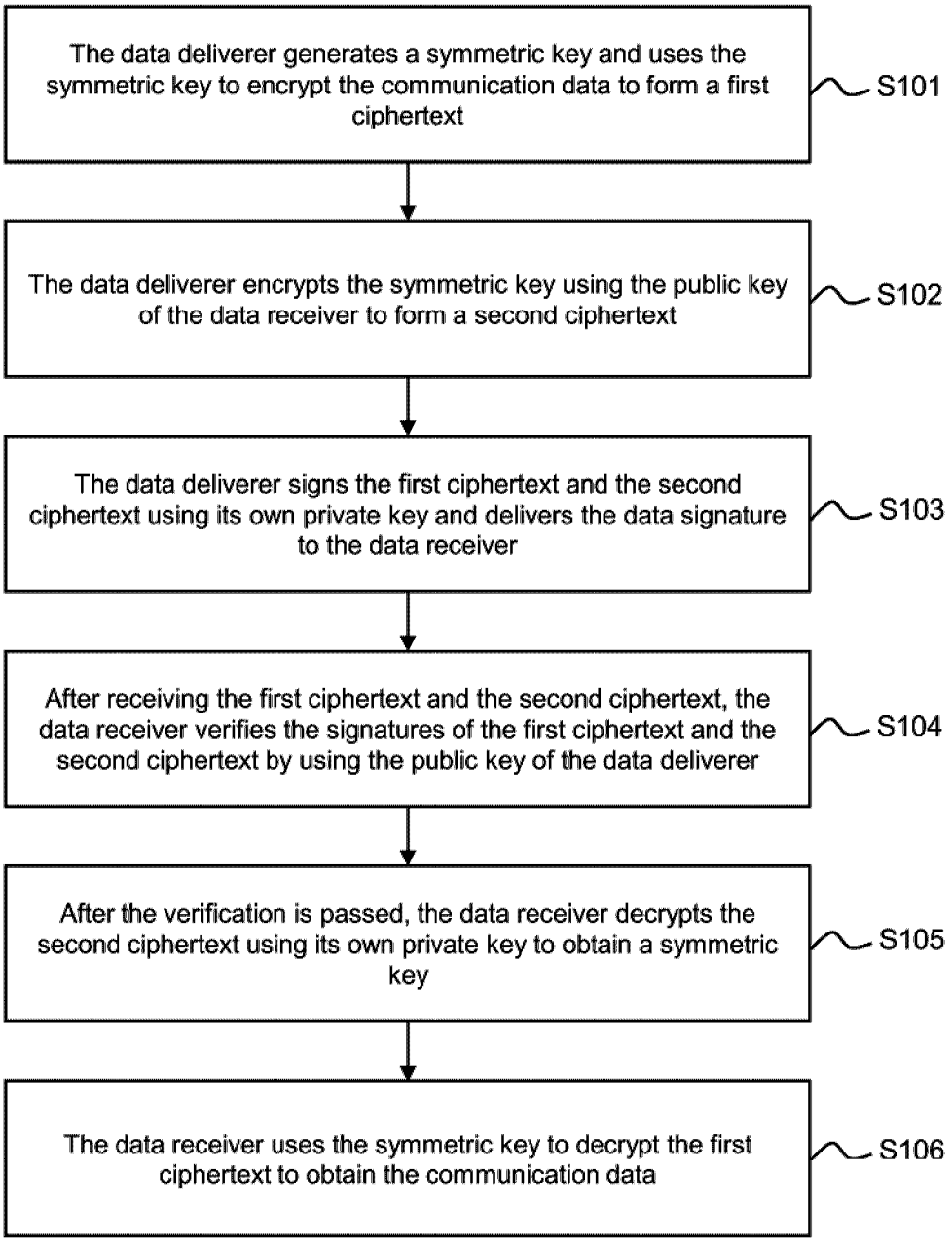


Figure 3

Date Reçue/Date Received 2020-07-14

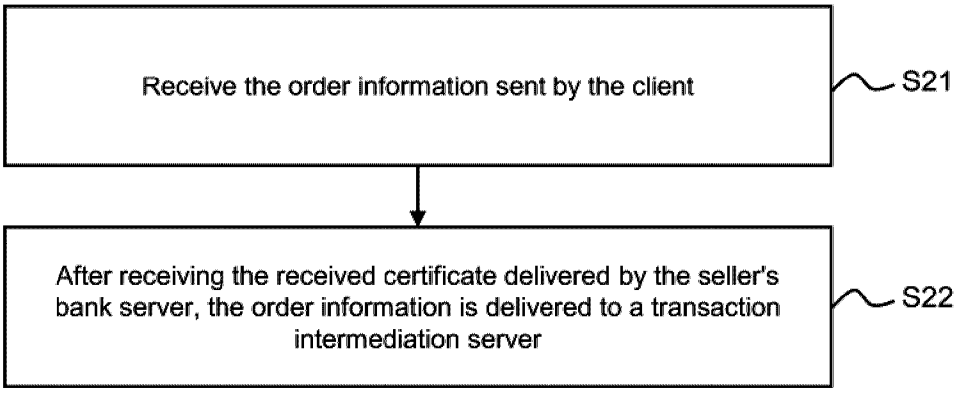


Figure 4

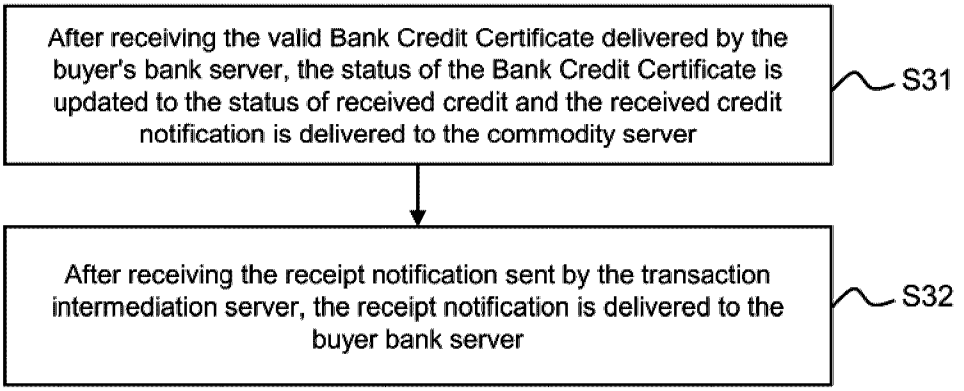


Figure 5

Date Reçue/Date Received 2020-07-14

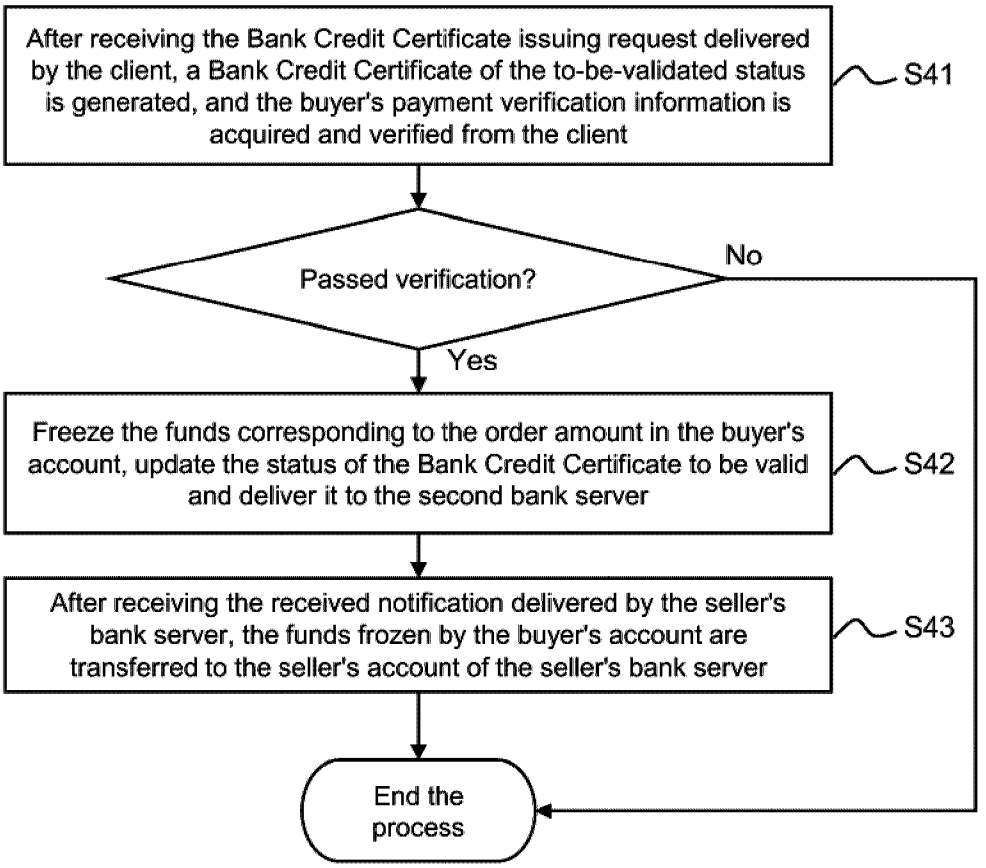


Figure 6

Date Reçue/Date Received 2020-07-14

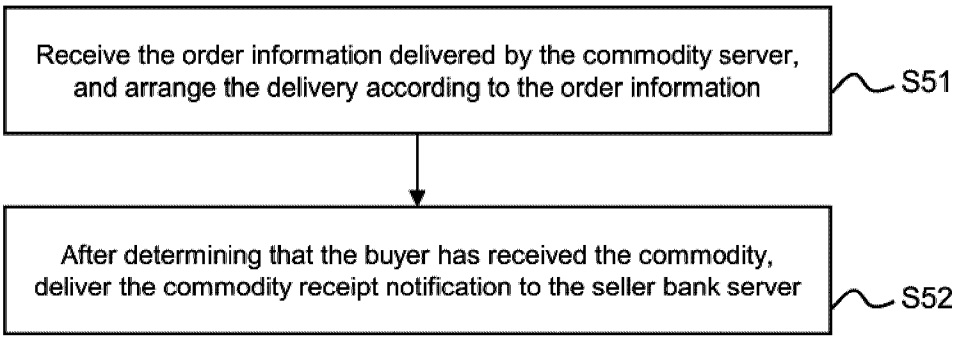


Figure 7

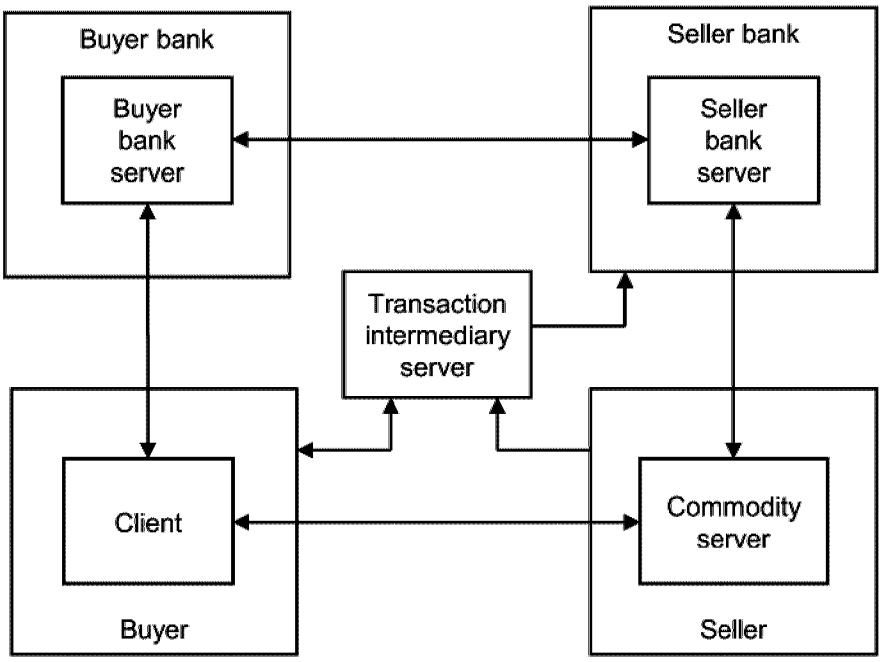


Figure 8

Date Reçue/Date Received 2020-07-14

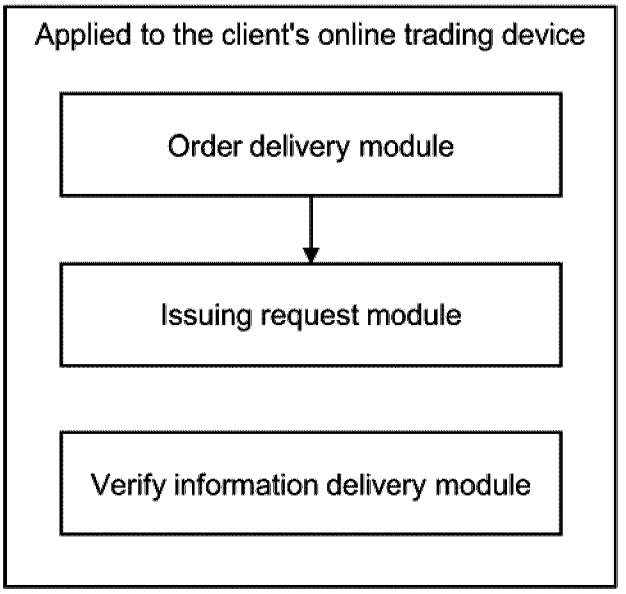


Figure 9

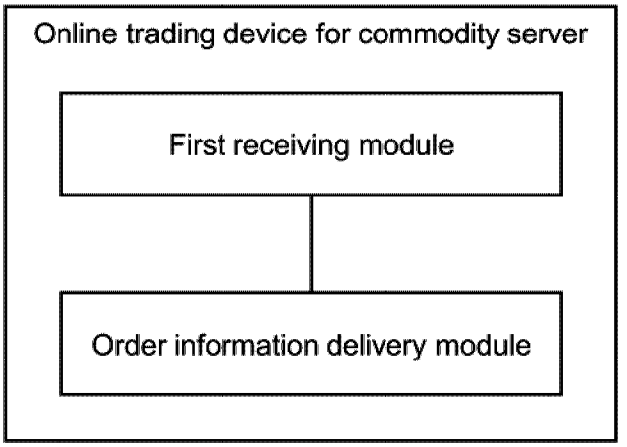


Figure 10

Date Reçue/Date Received 2020-07-14

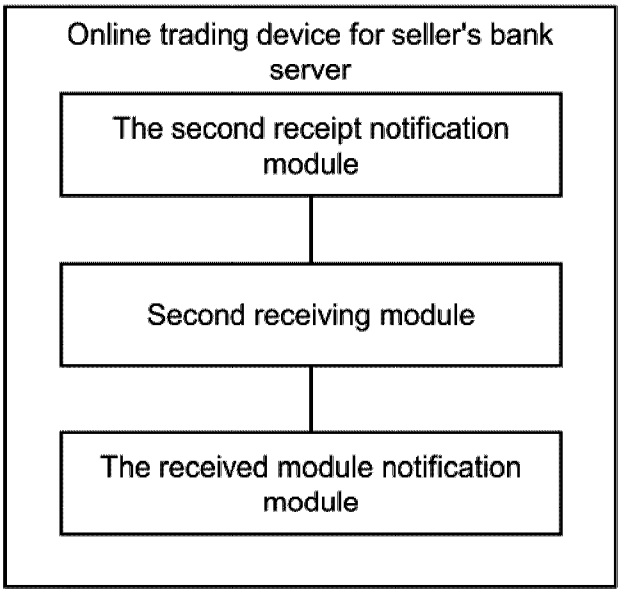


Figure 11

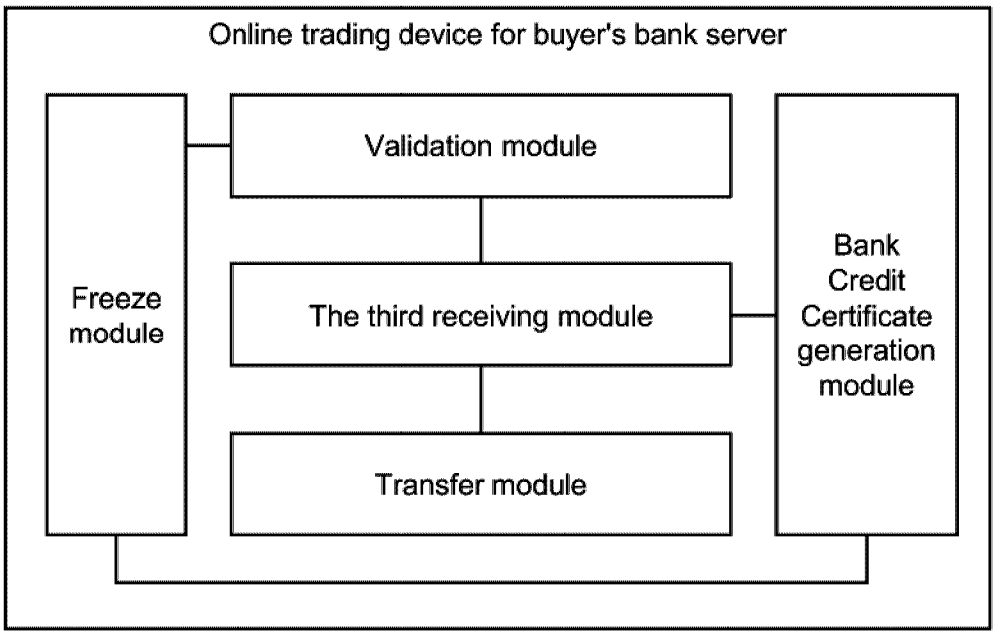


Figure 12

Date Reçue/Date Received 2020-07-14

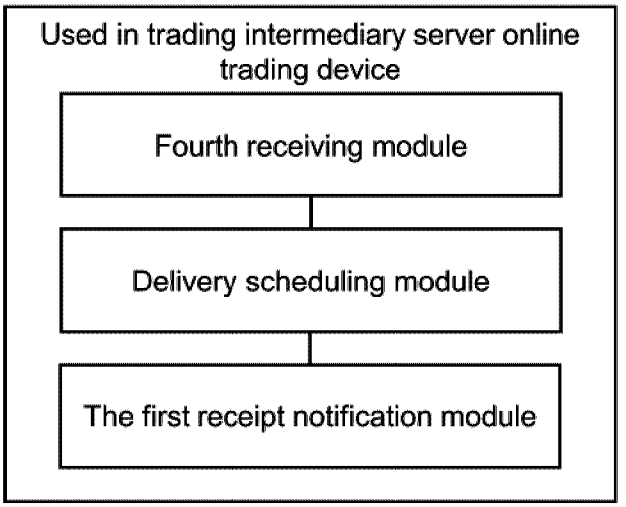


Figure 13

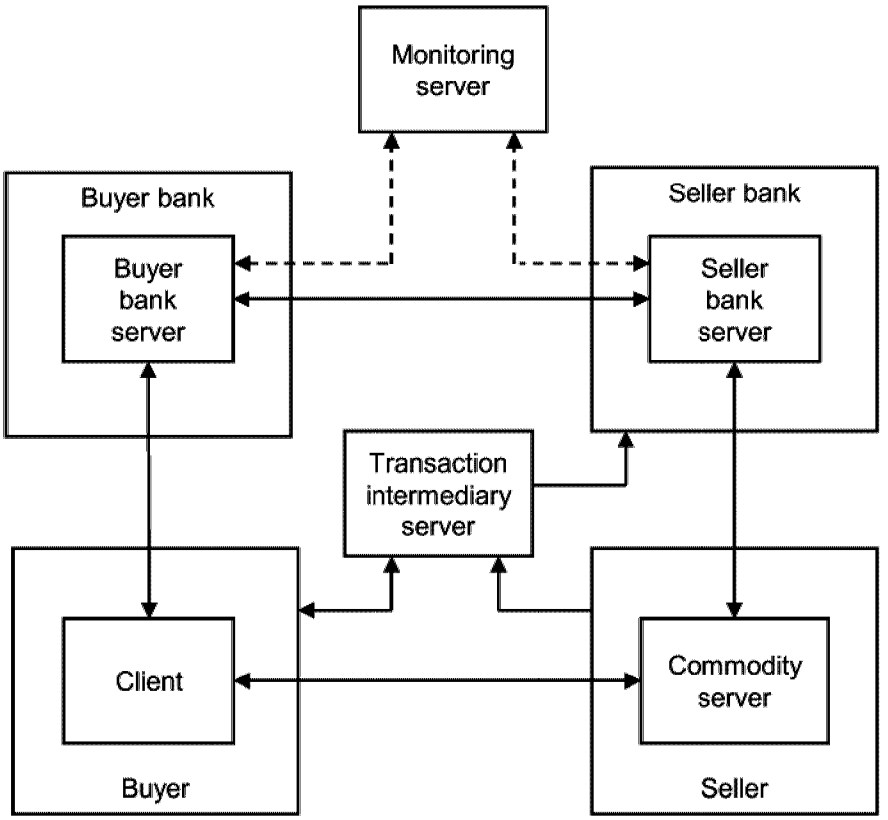
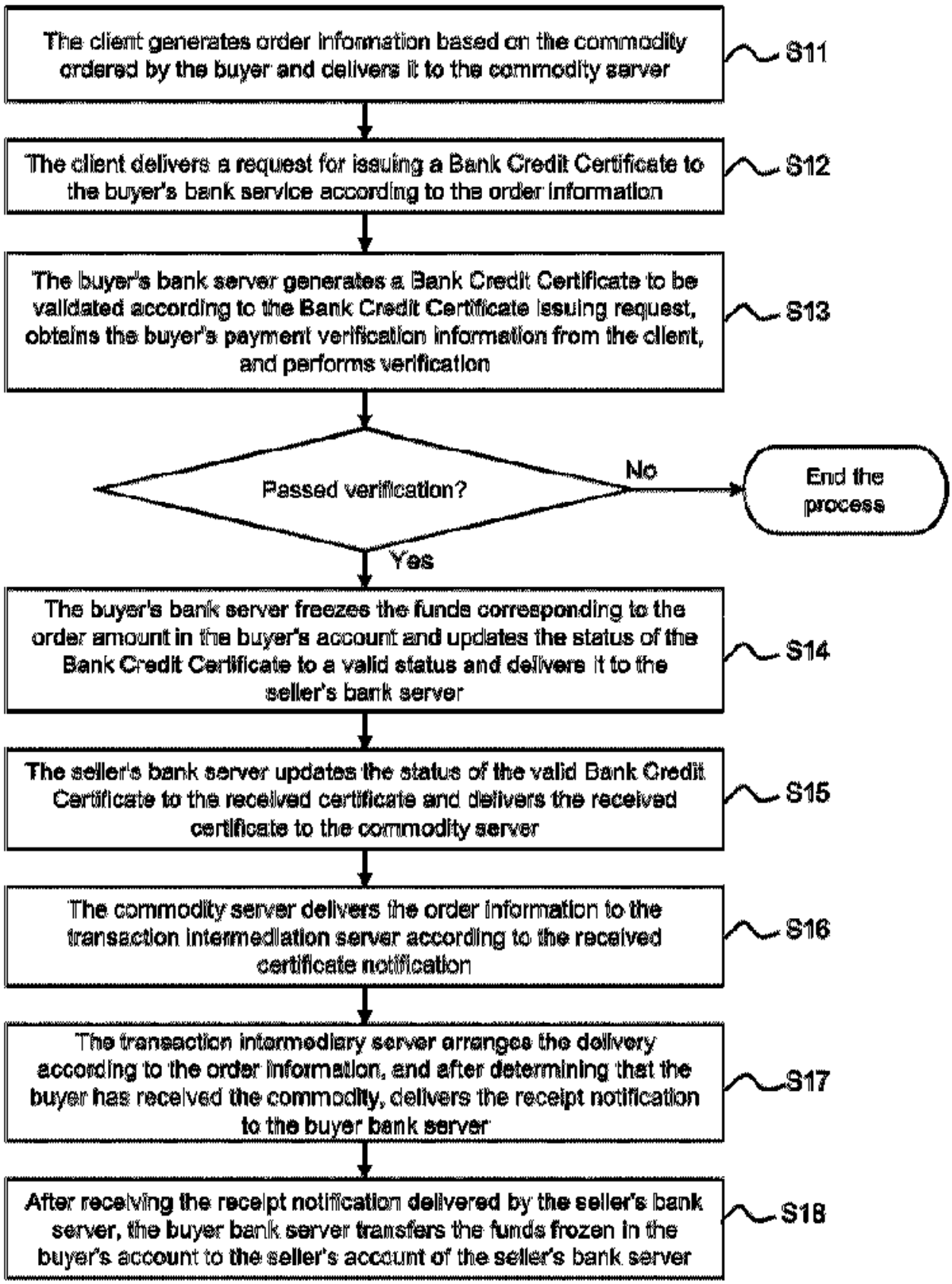


Figure 14

Date Reçue/Date Received 2020-07-14


The client generates order information based on the commodity ordered by the buyer and delivers it to the commodity server
S11
The client delivers a request for issuing a Bank Credit Certificate to the buyer's bank service according to the order information
S12
The buyer's bank server generates a Bank Credit Certificate to be validated according to the Bank Credit Certificate issuing request, obtains the buyer's payment verification information from the client, and performs verification
S13
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
S14
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
S15
The commodity server delivers the order information to the transaction intermediation server according to the received certificate notification
S16
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
S17
After receiving the receipt notification delivered by the seller's bank server, the buyer bank server transfers the funds frozen in the buyer's account to the seller's account of the seller's bank server
S18