(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 111835675 A
(43)申请公布日 2020.10.27

(21)申请号 201910297287.1

(22)申请日 2019.04.15

(71)申请人 宏碁股份有限公司
地址 中国台湾新北市

(72)发明人 林耕葆

(74)专利代理机构 深圳新创友知识产权代理有限公司 44223
代理人 江耀纯

(51)Int.Cl.
H04L 29/06(2006.01)

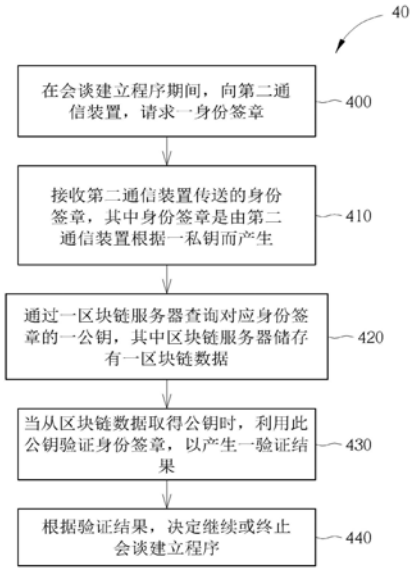
权利要求书3页 说明书6页 附图7页

(54)发明名称

验证网络通话身份的方法及相关装置

(57)摘要

本发明公开了一种验证网络通话身份的方法，用于支持一会谈启始协议及一区块链数据传输技术的一第一通信装置，该方法包含有：在一会谈建立程序期间，向该会谈建立程序中的一第二通信装置，请求一身份签章；接收该第二通信装置传送的该身份签章，其中该身份签章是由该第二通信装置根据一私钥而产生；通过一区块链服务器查询对应该身份签章的一公钥，其中该区块链服务器储存有一区块链数据；当从该区块链数据取得该公钥时，利用该公钥验证该身份签章，以产生一验证结果；以及根据该验证结果，决定继续或终止该会谈建立程序。



CN 111835675 A

1.一种验证网络通话身份的方法,用于支持一会谈启始协议(session initiation protocol,SIP)及一区块链数据传输技术(blockchain)的一第一通信装置,该方法包含有:

在一会谈建立程序期间,向该会谈建立程序中的一第二通信装置,请求一身份签章;

接收该第二通信装置传送的该身份签章,其中该身份签章是由该第二通信装置根据一私钥而产生;

通过一区块链服务器(block chain server)查询对应该身份签章的一公钥,其中该区块链服务器储存有一区块链数据;

当从该区块链数据取得该公钥时,利用该公钥验证该身份签章,以产生一验证结果;以及

根据该验证结果,决定继续或终止该会谈建立程序。

2.如权利要求1所述的方法,更包含有:

当从该区块链数据未取得该公钥时,结束或取消该会谈建立程序。

3.如权利要求1所述的方法,其特征在于,当从该区块链数据取得该公钥时,利用该公钥验证该身份签章,以产生该验证结果的步骤包含有:

利用该公钥解密该身份签章;

当该身分签章被成功解密,且解密后的该身分签章符合一默认规则时,判断该验证结果为成功;以及

当该身分签章未成功解密,或该身分签章被成功解密但不符合该默认规则时,判断该验证结果为失败。

4.如权利要求3所述的方法,其特征在于,根据该验证结果,决定继续或终止该会谈建立程序的步骤包含有:

当该验证结果为成功时,继续该会谈建立程序;以及

当该验证结果为失败时,结束或取消该会谈建立程序。

5.如权利要求2或4所述的方法,更包含有:

当结束或取消该会谈建立程序时,显示一警示信息予一用户。

6.如权利要求3所述的方法,其特征在于,该默认规则为关于该身份签章的一预设格式,该默认格式包含目标地址、来源地址、时间及会谈标识符的至少其中之一,以及该默认规则置入于该第二通信装置传送的该身份签章所附带的一明文数据中。

7.如权利要求6所述的方法,更包含有:

对该身份签章所附带的该明文数据,进行一检验,其中该检验步骤包含有:判断该明文数据是否符合一默认明文格式;

当该明文数据不符合该默认明文格式时,再次请求该第二通信装置传送该身份签章,或终止该会谈建立程序。

8.如权利要求7所述的方法,其特征在于,通过该区块链服务器查询对应该身份签章的该公钥的步骤包含有:

当该明文数据符合该默认明文格式时,通过该区块链服务器查询对应该身份签章的该公钥。

9.如权利要求1所述的方法,其特征在于,在该会谈建立程序期间,向该会谈建立程序中的该第二通信装置,请求该身份签章的步骤包含有:

传送该会谈启始协议或一超文本传输协议(hypertext transfer protocol,HTTP)的一请求信息至该第二通信装置,该请求信息用来指示该第二通信装置传送该身份签章给该第一通信装置。

10.如权利要求9所述的方法,其特征在于,该请求信息为会谈启始协议中的一邀请信息(INVITE)或一收讫确认信息(ACK)。

11.如权利要求1所述的方法,其特征在于,该第二通信装置传送的该身份签章附带有一明文数据,以及该方法更包含有:

对该明文数据,进行一检验,其中该检验步骤包含有:

判断该明文数据是否符合一默认明文格式;

当该明文数据不符合该默认明文格式时,再次请求该第二通信装置传送该身份签章,或终止该会谈建立程序。

12.如权利要求1所述的方法,其特征在于,通过该区块链服务器查询对应该身份签章的一公钥的步骤包含有:

传送一查询信息至该区块链服务器;

从该区块链服务器,接收包含该区块链数据的一回复信息;以及

从该区块链数据中,筛选出该公钥。

13.一种用来验证网络通话身份的一第一通信装置,该第一通信装置支持一会谈启始协议(session initiation protocol,SIP)及一区块链数据传输技术(blockchain),该通信装置包含有:

一处理单元,用来执行一程序代码;

一储存单元,耦接于该处理装置,用来储存该程序代码,其中该程序代码指示该处理单元执行以下步骤:

在一会谈建立程序期间,向该会谈建立程序中的一第二通信装置,请求一身份签章;

接收该第二通信装置传送的该身份签章,其中该身份签章是由该第二通信装置根据一私钥而产生;

通过一区块链服务器(block chain server)查询对应该身份签章的一公钥,其中该区块链服务器储存有一区块链数据;

当从该区块链数据取得该公钥时,利用该公钥验证该身份签章,以产生一验证结果;以及

根据该验证结果,决定继续或终止该会谈建立程序。

14.如权利要求13所述的第一通信装置,其特征在于,该程序代码更指示该处理单元执行以下步骤当从该区块链数据未取得该公钥时,结束或取消该会谈建立程序。

15.如权利要求13所述的第一通信装置,其特征在于,该程序代码更指示该处理单元执行以下步骤:

利用该公钥解密该身份签章;

当该身分签章被成功解密,且解密后的该身分签章符合一默认规则时,判断该验证结果为成功;以及

当该身分签章未成功解密,或该身分签章被成功解密但不符合该默认规则时,判断该验证结果为失败。

16.如权利要求15所述的第一通信装置,其特征在于,该程序代码更指示该处理单元执行以下步骤:

当判断该验证结果为成功时,继续该会谈建立程序;以及

当判断该验证结果为失败时,结束或取消该会谈建立程序。

17.如权利要求14或16所述的第一通信装置,其特征在于,该程序代码更指示该处理单元执行以下步骤:

当结束或取消该会谈建立程序时,显示一警示信息予一用户。

18.如权利要求13所述的第一通信装置,其特征在于,该程序代码更指示该处理单元执行以下步骤:

传送该会谈启始协议或一超文本传输协议(hypertext transfer protocol,HTTP)的一请求信息至该第二通信装置,该请求信息用来指示该第二通信装置传送该身份签章给该第一通信装置。

19.如权利要求13所述的第一通信装置,其特征在于,该程序代码更指示该处理单元执行以下步骤:

传送一查询信息至该区块链服务器;

从该区块链服务器,接收包含该区块链数据的一回复信息;以及

从该区块链数据中,筛选出该公钥。

20.一种用来验证网络通话身份的一第一通信装置,该第一通信装置包含有:一会谈启始协议单元,用来与一第二通信装置进行一会谈建立程序;

一身分签章请求单元,用来在该会谈建立程序期间,向该第二通信装置,请求一身份签章,以及用来接收该第二通信装置传送的该身份签章,其中该身份签章是由该第二通信装置根据一私钥而产生;

一区块链数据传输单元,用来向一区块链服务器查询对应该身份签章的一公钥,其中该区块链服务器储存有一区块链数据;以及

一身分签章验证单元,用来当该区块链数据传输单元从该区块链数据取得该公钥时,利用该身公钥验证该身份签章,以产生一验证结果。

21.如权利要求20所述的第一通信装置,其特征在于,该身份签章验证单元更用来:

利用该公钥解密该身份签章;

当该身分签章被成功解密,且解密后的该身分签章符合一默认规则时,判断该验证结果为成功;以及

当该身分签章未成功解密,或该身分签章被成功解密但不符合该默认验证规则时,判断该验证结果为失败。

22.如权利要求21所述的第一通信装置,其特征在于,该身分签章验证单元更用来当该验证结果成功时,指示该会谈启始协议单元继续该会谈建立程序,以及当该验证结果失败时,指示该会谈启始协议单元结束或取消该会谈建立程序。

23.如权利要求20所述的第一通信装置,其特征在于,该区块链数据传输单元更用来:

传送一查询信息至该区块链服务器;

从该区块链服务器,接收包含该区块链数据的一回复信息;以及

从该区块链数据中,筛选出该公钥。

验证网络通话身份的方法及相关装置

技术领域

[0001] 本发明涉及一种验证网络通话身份的方法及相关装置，尤指一种基于区块链数据传输技术来验证网络通话身份的方法及相关装置。

背景技术

[0002] 会谈启始协议(Session Initiation Protocol，SIP)是一种网络通信协议，为VoIP网络电话技术中较主流的协议。会谈启始协议在会谈建立程序中，定义有六种信息：注册(REGISTER)、邀请(INVITE)、收讫确认(ACK)、取消(CANCEL)、结束(BYE)及查询(OPTIONS)。请参见第1图，其为习知一会谈建立程序的示意图。当发话端欲建立会谈时，发话端向受话端传送邀请信息至受话端，直至传送收讫确认信息后，即可开始串流通话。

[0003] 在多数情境中，发话端不会知道受话端当前的IP地址，因此，大多会向代理服务器(Proxy Server)请求转发信息，其中代理服务器储存有向其注册的用户账号及对应的IP地址，因此具有路由功能。如第2图所示，发话端传送邀请信息至代理服务器，接着代理服务器将邀请信息传送至受话端，进而实现两方会谈建立。由上述可知，在会谈启始协议架构下，发话端与受话端之间会通过网络电话的服务商与其服务器，来建立会谈。然而，若是服务器遭骇，或是用户的账号密码泄漏等问题发生，可能导致发话端或受话端实际上并非其本人。

发明内容

[0004] 因此，本发明的主要目的即在于提供一种验证网络通话身份的方法及相关装置，以解决上述问题。

[0005] 本发明公开一种验证网络通话身份的方法，用于支持一会谈启始协议及一区块链数据传输技术的一第一通信装置，该方法包含有：在一会谈建立程序期间，向该会谈建立程序中的一第二通信装置，请求一身份签章；接收该第二通信装置传送的该身份签章，其中该身份签章是由该第二通信装置根据一私钥而产生；通过一区块链服务器查询对应该身份签章的一公钥，其中该区块链服务器储存有一区块链数据；当从该区块链数据取得该公钥时，利用该公钥验证该身份签章，以产生一验证结果；以及根据该验证结果，决定继续或终止该会谈建立程序。

[0006] 本发明另公开一种用来验证网络通话身份的一第一通信装置，该第一通信装置支持一会谈启始协议及一区块链数据传输技术，该通信装置包含有：一处理单元，用来执行一程序代码；一储存单元，耦接于该处理装置，用来储存该程序代码，其中该程序代码指示该处理单元执行以下步骤：在一会谈建立程序期间，向该会谈建立程序中的一第二通信装置，请求一身份签章；接收该第二通信装置传送的该身份签章，其中该身份签章是由该第二通信装置根据一私钥而产生；通过一区块链服务器查询对应该身份签章的一公钥，其中该区块链服务器储存有一区块链数据；当从该区块链数据取得该公钥时，利用该公钥验证该身份签章，以产生一验证结果；以及根据该验证结果，决定继续或终止该会谈建立程序。

[0007] 本发明另公开一种用来验证网络通话身份的一第一通信装置，该第一通信装置包

含有:一会谈启始协议单元,用来与一第二通信装置进行一会谈建立程序;一身分签章请求单元,用来在该会谈建立程序期间,向该第二通信装置,请求一身份签章,以及用来接收该第二通信装置传送的该身份签章,其中该身份签章是由该第二通信装置根据一私钥而产生;一区块链数据传输单元,用来向一区块链服务器查询对应该身份签章的一公钥,其中该区块链服务器储存有一区块链数据;以及一身分签章验证单元,用来当该区块链数据传输单元从该区块链数据取得该公钥时,利用该身公钥验证该身份签章,以产生一验证结果。

附图说明

[0008] 图1-2为习知一会谈建立程序的示意图。

[0009] 图3为本发明实施例一通信装置的示意图。

[0010] 图4为本发明实施例一网络通话身份验证流程的示意图。

[0011] 图5为本发明实施例一通信装置的应用架构图。

[0012] 图6为本发明实施例一网络通话身份验证流程的示意图。

[0013] 图7-8为本发明实施例一网络通话身份验证程序的示意图。

[0014] 其中,附图标记说明如下:

[0015]	30、50	通信装置
[0016]	300	处理单元
[0017]	310	储存单元
[0018]	320	通信接口单元
[0019]	314	程序代码
[0020]	40、60	流程
[0021]	400-440、601-607	步骤
[0022]	501	会谈启始协议单元
[0023]	502	身分签章请求单元
[0024]	503	身分签章验证单元
[0025]	504	区块链数据传输单元
[0026]	505	警示信息显示单元

具体实施方式

[0027] 请参考图3,图3为本发明实施例一通信装置30的示意图。通信装置30可为图1-2所示的发话端/受话端或代理服务器。详细来说,通信装置30包含有一处理单元300、一储存单元310以及一通信接口单元320。处理单元300可为一微处理器或一特殊应用集成电路(application-specific integrated circuit,ASIC)。储存单元310可为任一数据储存装置,用来储存一程序代码314,并通过处理单元300读取及执行程序代码314。举例来说,储存单元310可为用户识别模块(subscriber identity module,SIM)、只读式内存(read-only memory,ROM)、随机存取内存(random-access memory,RAM)、光盘只读存储器(CD-ROMs)、磁带(magnetic tapes)、软盘(floppy disks)、光学数据储存装置(optical data storage devices)等等,而不限于此。通信接口单元320通过无线通信方式,用来与另一通信装置交换讯号。

[0028] 本案通信装置30在会谈启始协议(Session Initiation Protocol,SIP)架构下,支持区块链数据传输技术(blockchain)及非对称式加密与数字签名(DigitalSignature)。非对称式加密也就是一般常见的公私钥加密,公钥加密的内容只有私钥能解密,反之,私钥加密的内容只有公钥能解密。数字签名是公私钥的一种应用,用于验证文件的发送者确实是其本人。因此本发明采用数字签名技术,于SIP通话过程中验证双方身份。简单来说,数字签名就是用发送者的私钥加密文件,接收者再用发送者的公钥解密文件。一般应用情境中,通过数字签名签署发送的文件内容会附带明文数据,以供接收者验证文件内容,但若文件内容是固定或可预期的,那么也可以不附带明文数据。

[0029] 区块链是一群分散的客户端节点,并由所有参与者组成的分布式数据库,任何人都可以通过公开的接口去查询区块链中的数据,系统数据非常透明。区块链的另一大特色是其「不可窜改性」,区块链中的每一笔数据一旦写入就不可以再改动,只要数据被验证完就永久的写入该区块中。此外,每个客户端节点的区块链数据都相同,也让区块链中的数据若被窜改时,容易被发现。

[0030] 值得注意的是,一般的SIP通话依赖可信赖的第三方(如代理服务器)做身份验证与媒合,因此在SIP通话的数据传递过程中,可能会发生伪装服务器、窜改封包等的资安问题。由上述可知,区块链本身具有去中心化的特性(即去中心化的分布式数据库),也就是弱化对信赖的第三方的依赖,因此本案基于区块链的网络通话身份验证机制,能加强网络通话的安全。详细来说,区块链的分布式特性让攻击者难以针对特定服务器伪装,且区块链的不可窜改性也让攻击者难以达到窜改区块链数据的目的,因而本发明提出通过区块链来纪录公钥的概念。由于通信装置30是自行从区块链上获取公钥,而非通过通话数据中传递,因此黑客将难以通过假冒数字签名与公钥的方式进行攻击。因此,本发明能实现SIP通话的身份验证,并强化通话数据传递的安全性。

[0031] 请参考图4,其为本发明实施例一网络通话身份验证流程40的示意图。网络通话身份验证流程40用于图3所示的通信装置30(在本文中称为第一通信装置)。网络通话身份验证流程40可编译为程序代码314,并包含有以下步骤:

[0032] 步骤400:在会谈建立程序期间,向第二通信装置,请求一身份签章。

[0033] 步骤410:接收第二通信装置传送的身份签章,其中身份签章是由第二通信装置根据一私钥而产生。

[0034] 步骤420:通过一区块链服务器查询对应身份签章的一公钥,其中区块链服务器储存有一区块链数据。

[0035] 步骤430:当从区块链数据取得公钥时,利用此公钥验证身份签章,以产生一验证结果。

[0036] 步骤440:根据验证结果,决定继续或终止会谈建立程序。

[0037] 根据流程40,第一通信装置在会谈建立程序期间(以下称为SIP通话),如发起或接收到邀请信息(INVITE)时,首先请求第二通信装置传送身份签章(即通过私钥加密的信息)。当第一通信装置接收到第二通信装置回复的身分签章时,第一通信装置会自行通过区块链来查询对应此身份签章的公钥,以验证第二通信装置的身份,进而决定要继续或终止SIP通话。举例来说,当第一通信装置从区块链查询到公钥时,利用此公钥来解密第二通信装置传送的身份签章。若此公钥能成功解密身分签章,则能确认第二通信装置的身份,因此

第一通信装置会继续SIP通话，如传送收讫确认信息至第二通信装置，以完成SIP通话。相反的，若此公钥不能成功解密身分签章，第一通信装置会终止SIP通话，如传送结束信息或取消信息至第二通信装置。此外，当第一通信装置从区块链未查询到公钥时，第一通信装置会终止SIP通话。

[0038] 进一步地，第一通信装置请求第二通信装置的身份签章的方式为传送会谈启始协议或超文本传输协议(hypertext transfer protocol，HTTP)中的一请求信息至第二通信装置，此请求信息用来指示第二通信装置传送身份签章至第一通信装置。在一实施例中，请求信息可为会谈启始协议中的邀请信息或收讫确认信息(ACK)。

[0039] 换句话说，本发明默认区块链上纪录有通信装置的公钥，公钥可由通信装置或账号管理的主机/服务器产生并上传到区块链，而对应的私钥则由通信装置自行保存，以供通信装置能够利用私钥签署发送身份签章，而欲验证身份签章的通信装置则从区块链取得公钥来解密身份签章，进而验证通信装置的身份。

[0040] 图5为本发明实施例一通信装置50的应用架构图。通信装置50包含有会谈启始协议单元501、身分签章请求单元502、身分签章验证单元503、区块链数据传输单元504及警示信息显示单元505。会谈启始协议单元501用来与另一通信装置进行SIP通话，并可呼叫身分签章请求单元502向另一通信装置请求身份签章。在一实施例中，身分签章请求单元502可监听会谈启始协议单元501，并自行决定向另一通信装置请求身份签章。区块链数据传输单元504主要处理区块链数据传输，可以仅储存区块链的标头等轻量数据，有简易的交易验证功能，比如区块链的轻量节点(Lightweight Client)用来向区块链服务器(储存有可供查取的、同步的且完整的区块链数据，比如类型为完整节点(Full Node)的区块链节点)查询对应身份签章的公钥。身分签章验证单元503用来当区块链数据传输单元504从区块链数据取得公钥时，利用公钥验证身份签章，产生一验证结果。进一步地，身份签章验证单元503可根据验证结果，呼叫会谈启始协议单元501继续或终止SIP通话。举例来说，若验证结果为成功，身分签章验证单元503呼叫会谈启始协议单元501继续SIP通话。另一方面，若验证结果为失败，身分签章验证单元503呼叫会谈启始协议单元501终止SIP通话，并同时呼叫警示信息显示单元505显示一警示信息予用户。

[0041] 本发明的通信装置50(以下称为第一通信装置)的运作方式可归纳为网络通话身份验证流程60，如图6所示。第一通信装置的会谈启始协议单元传送/接收邀请信息或会谈启始协议中的后续信息(步骤601)，接着身分签章请求单元向第二通信装置请求身分签章，并等待接收身分签章(步骤602)。若身分签章请求单元未成功接收身分签章，则身分签章请求单元可再次向第二通信装置请求身分签章(步骤603a)，或者指示会谈启始协议单元终止SIP通话，以及指示警示信息显示单元显示警示信息(步骤603b)。相反的，若身分签章请求单元成功接收身分签章，身分签章请求单元将接收到的身分签章传送给身分签章验证单元，以对身分签章所附带的明文数据，进行初步检验(步骤604)。初步检验方式可为判断明文数据是否符合默认明文格式要求，但不限于此。此外，若身分签章未附带明文数据，则此初步检验步骤可省略。若明文数据符合默认明文格式要求时，身分签章验证单元判断初步检验成功，并指示区块链数据传输单元向区块链服务器查询并取得预先储存于区块链上的公钥(步骤605)。反之，若明文数据不符合默认明文格式要求时，身分签章验证单元判断初步检验失败，并指示身分签章请求单元再次向第二通信装置请求身分签章(步骤603a)，或

者指示会谈启始协议单元终止SIP通话,以及指示警示信息显示单元显示警示信息(步骤603b)。

[0042] 当区块链数据传输单元从区块链服务器的区块链上取得公钥时,会将此公钥传送至身分签章验证单元,以供身分签章验证单元验证/解密身分签章(步骤606)。在一实施例中,若身分签章被成功解密,且解密后的身分签章内容符合默认格式/规则时,身分签章验证单元指示会谈启始协议单元继续SIP通话(步骤607);若身分签章未被成功解密,或身分签章成功解密,但解密后的身分签章内容不符合默认格式/规则时,身分签章验证单元指示会谈启始协议单元终止SIP通话,并指示警示信息显示单元显示警示信息(步骤603b)。另一方面,当区块链数据传输单元未从区块链服务器的区块链上取得公钥时,区块链数据传输单元亦指示会谈启始协议单元终止SIP通话,并指示警示信息显示单元显示警示信息(步骤603b)。

[0043] 在一实施例中,默认格式包含目标地址、来源地址、时间及会谈标识符的至少其中之一,以及默认规则可置入于身份签章所附带的明文数据中。举例来说,身分签章验证单元利用取得的公钥解密身分签章,并得出以下身分签章内容:

[0044] From:7933@voip.acer.com

[0045] To:0001@voip.acer.com

[0046] Time:1528037983

[0047] InviteId:123456789

[0048] 当身分签章内容符合通信装置的默认格式时,则通信装置判断此身份签章验证成功,并继续SIP通话;反之,通信装置判断身分签章验证失败,终止SIP通话。

[0049] 值得注意的是,网络通话身份验证流程60可由邀请信息或后续信息(如收讫确认信息或后续其他信息)的传送/接收来触发。若在传送/接收邀请信息的阶段就进行网络通话身份验证,则可以用于检验包含代理服务器的身份,而若在传送/接收收讫确认信息阶段进行网络通话身份验证,则可以只验证实际通话装置(即第二通信装置)的身份。于哪一阶段开始检验网络通话身份可由第一通信装置的应用程序的需求来决定。

[0050] 值得注意的是,不论发话端与受话端,或是代理服务器都是在SIP通话中的通信装置,因此都可相互请求对方给予身份签章,身份签章由对方通信装置使用保存的私钥签署发送,此时区块链上纪录有对应此私钥的公钥。

[0051] 详细来说,区块链数据传输单元向区块链服务器查询并取得预先储存于区块链上的公钥的方式可参见图7-8。图7-8为本发明实施例一通信装置之间的网络通话身份验证的示意图。如图7所示,第一通信装置向第二通信装置传送邀请信息,第二通信装置向第一通信装置请求身份签章并接收回传的身份签章。接着,第二通信装置传送「查询区块录交易信息」的查询信息至区块链服务器,因此区块链服务器回传「返回区块链交易信息」的回复信息至第二通信装置。第二通信装置从「返回区块链交易信息」,查询交易信息并过滤找出符合的数据,最终筛选出公钥。本发明筛选找出公钥的方式,在此不做限制。

[0052] 此外,在筛选找出公钥后,第二通信装置利用此公钥验证身分签章。假设身分签章验证结为为失败,第二通信装置传送结束信息或取消信息至第一通信装置,以立即终止SIP通话,并藉由用户接口或纯文本等方式显示警示信息,告知用户刚刚的SIP通话对象验证失败。

[0053] 在一实施例中，本发明通过区块链纪录公钥数据的方式，亦可应用于比特币区块链的交易场景中，用来读取区块链中的公钥数据，进而验证比特币交易者的身份。

[0054] 上述所有步骤，包含所建议的步骤，可通过硬件、韧体(即硬件装置与计算机指令的组合，硬件装置中的数据为只读软件数据)或电子系统等方式实现。举例来说，硬件可包含模拟、数字及混合电路(即微电路、微芯片或硅芯片)。电子系统可包含系统单芯片(system on chip,SOC)、系统封装

[0055] (system in package,Sip)、计算机模块(computer on module,COM)及通信装置30。

[0056] 综上所述，本发明架构于SIP标准上运作，并通过区块链纪录公钥数据，因此能验证SIP通话身份。详细来说，通信装置读取区块链中的公钥数据，来解密身份签章，以确认对方通信装置的身份。值得注意的是，将区块链的特性用于网络通话的身份验证，能强化网络通话的信息安全，使通话双方的网络通话质量与信赖更受保障。

[0057] 以上所述仅为本发明的优选实施例而已，并不用于限制本发明，对于本领域的技术人员来说，本发明可以有各种更改和变化。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

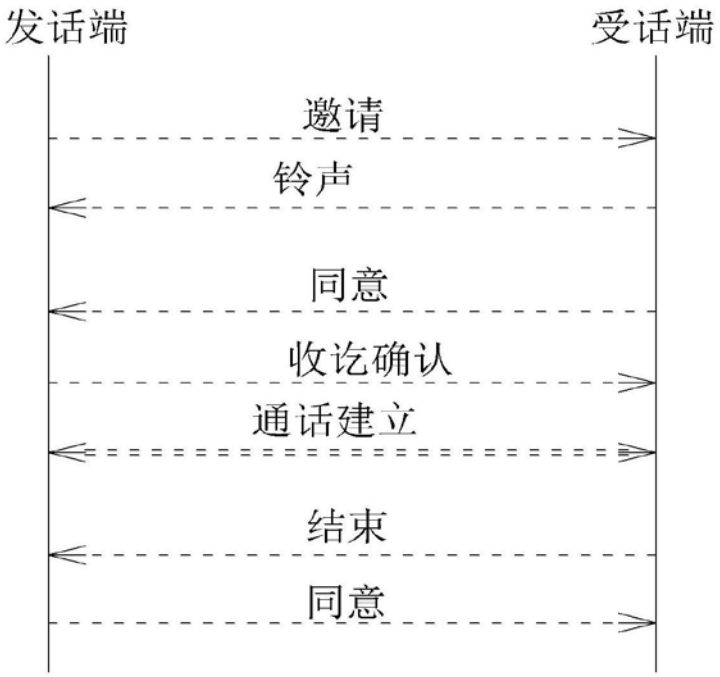

发话端
受话端
邀请
铃声
同意
收讫确认
通话建立
结束
同意

图1

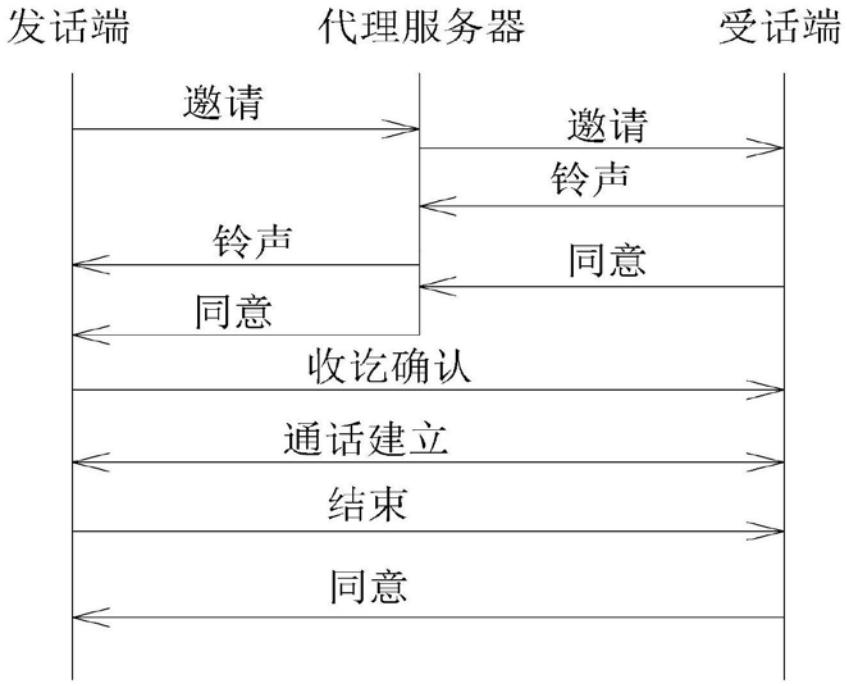

发话端
代理服务器
受话端
邀请
邀请
铃声
铃声
同意
同意
收讫确认
通话建立
结束
同意

图2

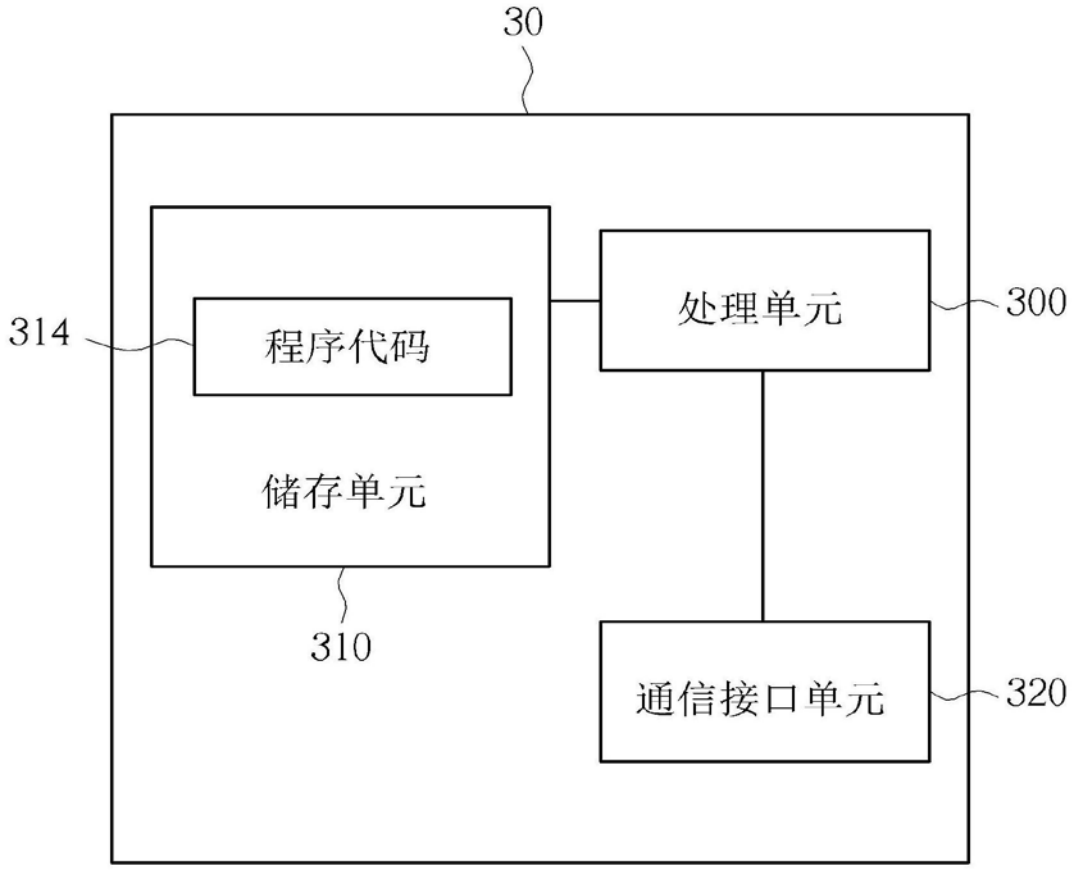


图3

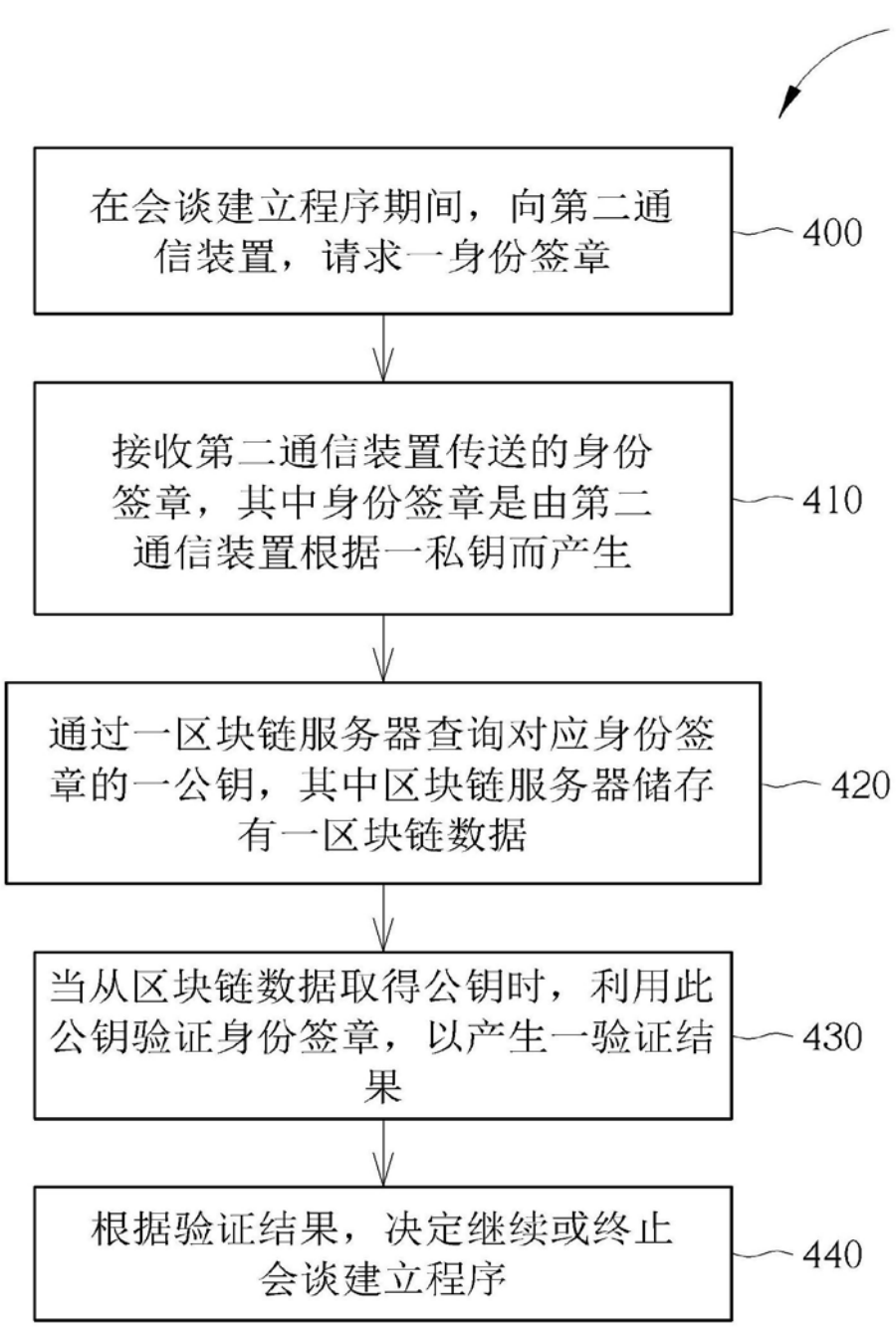

40
在会谈建立程序期间，向第二通信装置，请求一身份签章
400
接收第二通信装置传送的身份签章，其中身份签章是由第二通信装置根据一私钥而产生
410
通过一区块链服务器查询对应身份签章的一公钥，其中区块链服务器储存有一区块链数据
420
当从区块链数据取得公钥时，利用此公钥验证身份签章，以产生一验证结果
430
根据验证结果，决定继续或终止会谈建立程序
440

图4

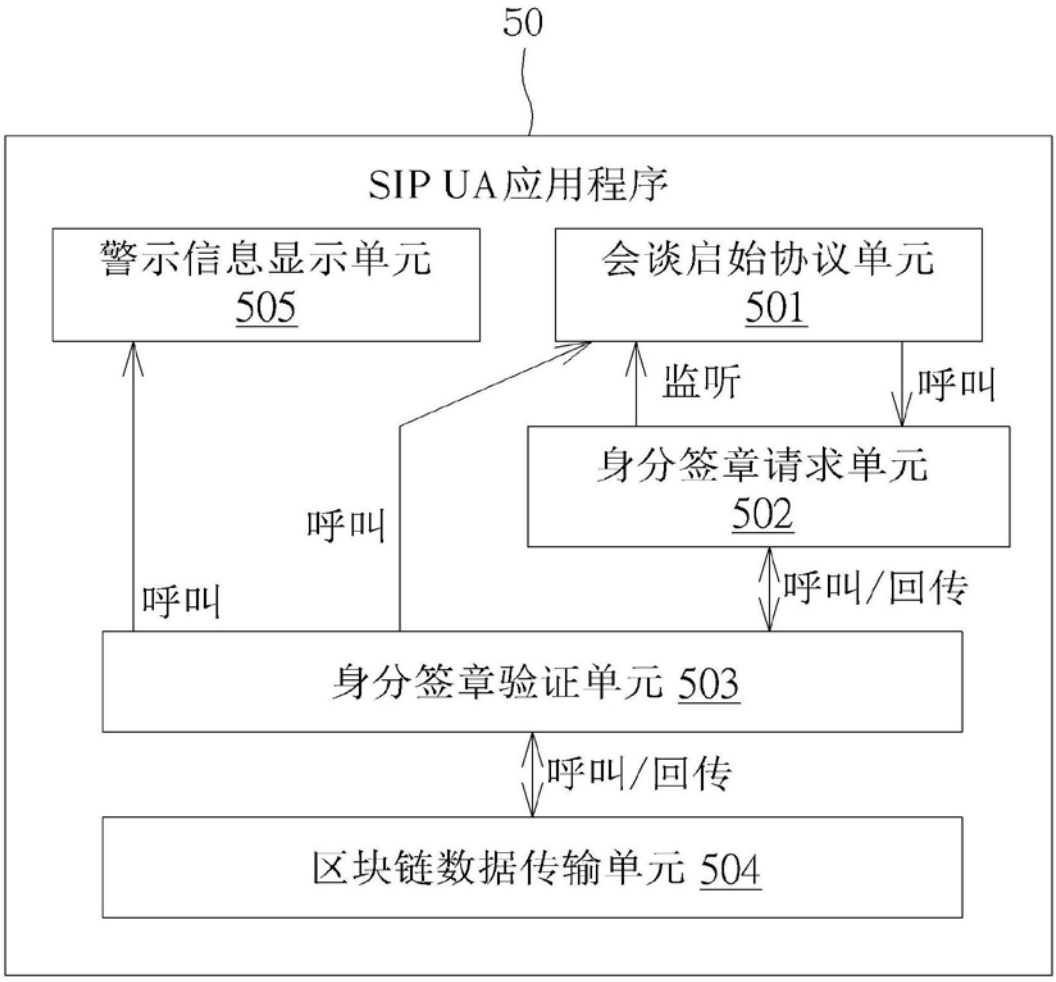

50
SIP UA应用程序
警示信息显示单元
505
会谈启始协议单元
501
监听
呼叫
身分签章请求单元
502
呼叫
呼叫
呼叫/回传
身分签章验证单元 503
呼叫/回传
区块链数据传输单元 504

图5

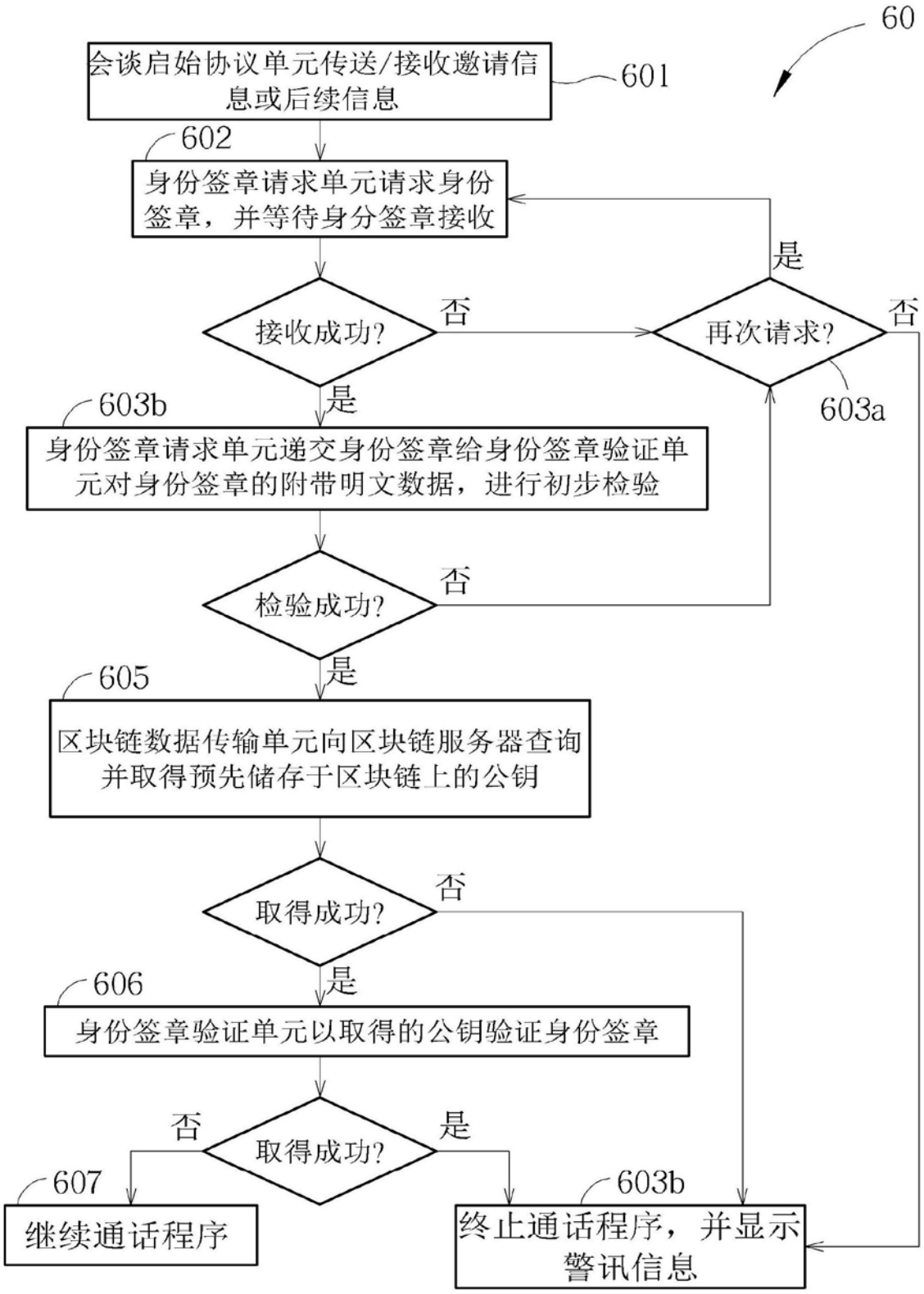

60
会谈启始协议单元传送/接收邀请信息或后续信息
601
602
身份签章请求单元请求身份签章，并等待身分签章接收
接收成功?
否
是
再次请求?
否
是
603a
603b
身份签章请求单元递交身份签章给身份签章验证单元对身份签章的附带明文数据，进行初步检验
检验成功?
否
是
605
区块链数据传输单元向区块链服务器查询并取得预先储存于区块链上的公钥
取得成功?
否
是
606
身份签章验证单元以取得的公钥验证身份签章
取得成功?
否
是
607
继续通话程序
603b
终止通话程序，并显示警讯信息

图6

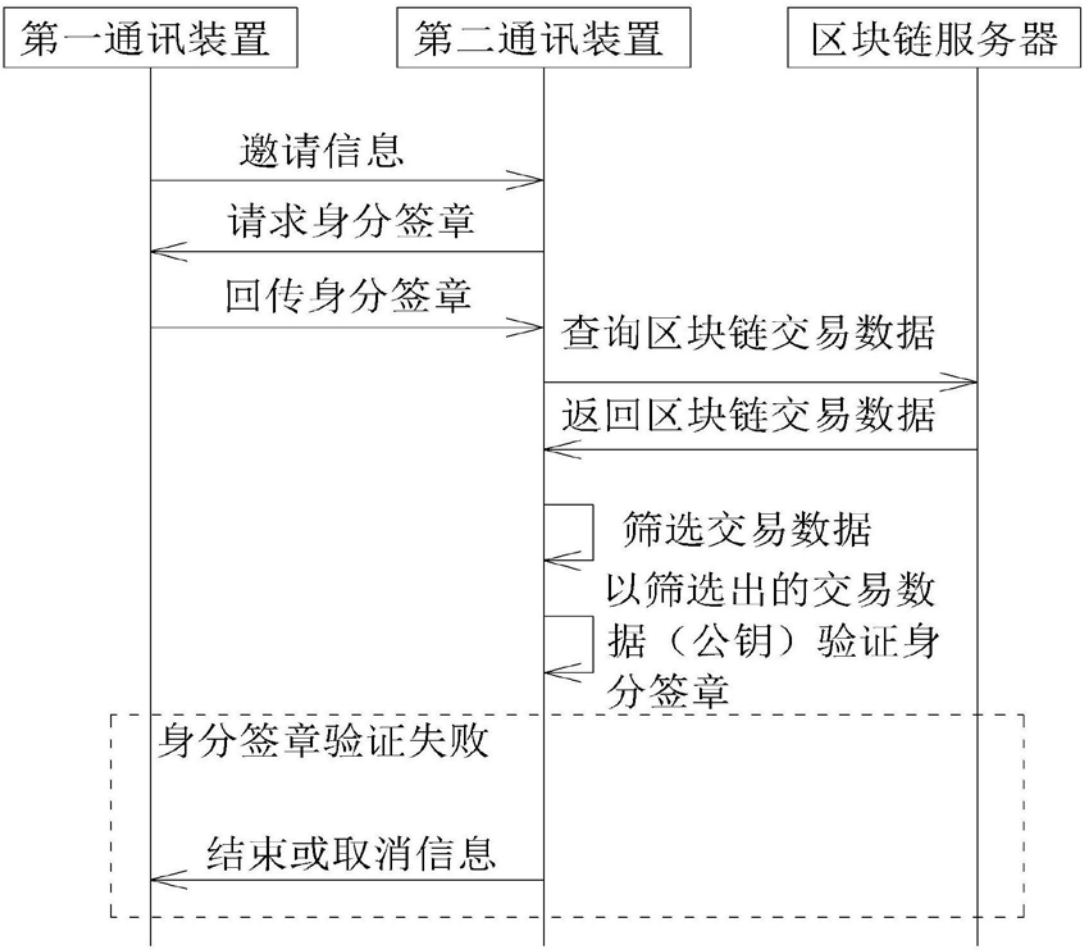

第一通讯装置
第二通讯装置
区块链服务器
邀请信息
请求身分签章
回传身分签章
查询区块链交易数据
返回区块链交易数据
筛选交易数据
以筛选出的交易数据（公钥）验证身分签章
身分签章验证失败
结束或取消信息

图7

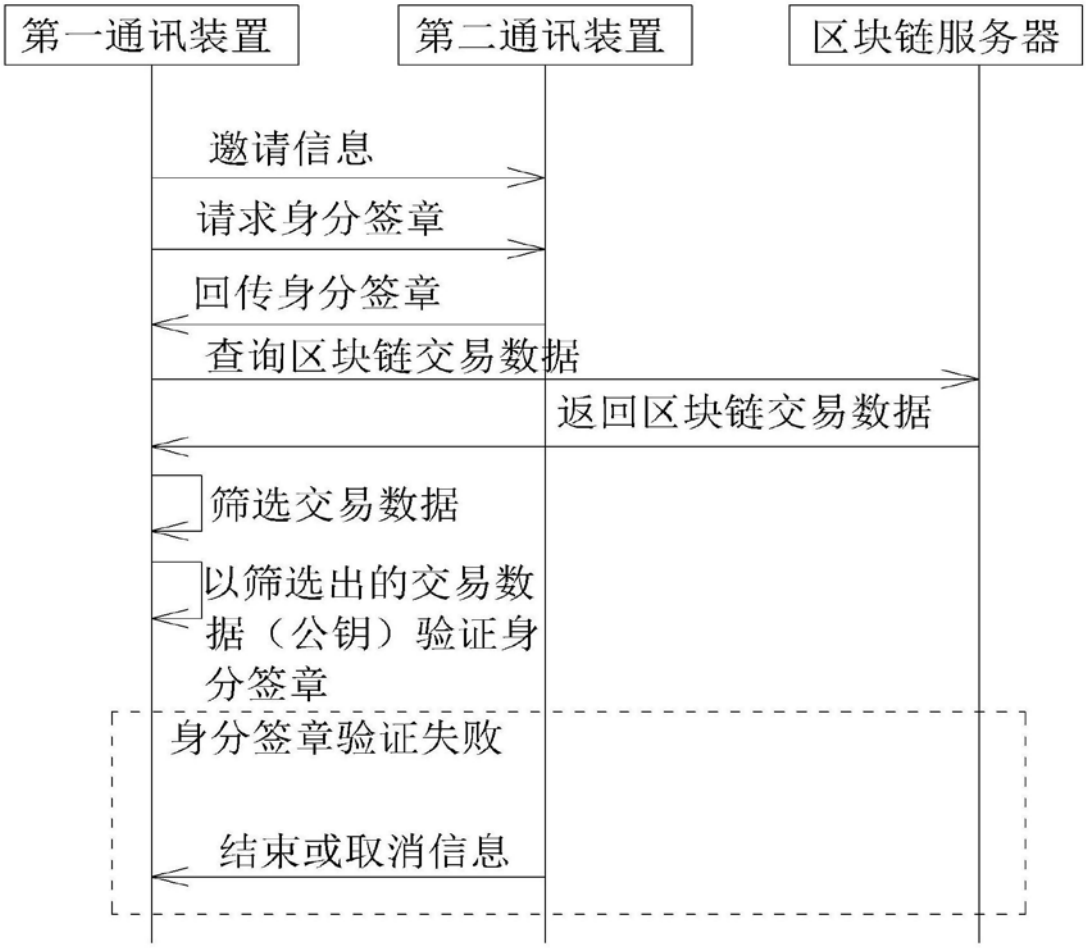

第一通讯装置
第二通讯装置
区块链服务器
邀请信息
请求身分签章
回传身分签章
查询区块链交易数据
返回区块链交易数据
筛选交易数据
以筛选出的交易数据（公钥）验证身分签章
身分签章验证失败
结束或取消信息

图8