



(12)发明专利申请

(10)申请公布号 CN 107493162 A

(43)申请公布日 2017.12.19

(21)申请号 201710613402.2

(22)申请日 2017.07.25

(71)申请人 中国联合网络通信集团有限公司

地址 100033 北京市西城区金融大街21号

(72)发明人 田新雪 马书惠

(74)专利代理机构 北京同立钧成知识产权代理有限公司 11205

代理人 张子青 刘芳

(51)Int.Cl.

H04L 9/06(2006.01)

H04L 9/08(2006.01)

H04L 9/32(2006.01)

G06Q 20/32(2012.01)

G06Q 20/38(2012.01)

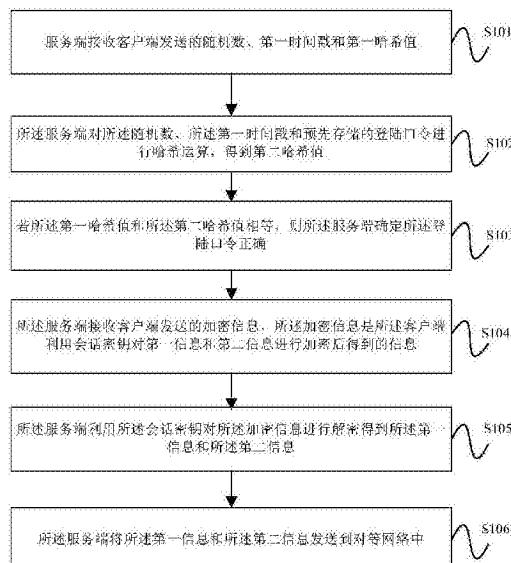
权利要求书2页 说明书6页 附图3页

(54)发明名称

区块链节点的实现方法及装置

(57)摘要

本发明实施例提供一种区块链节点的实现方法及装置。该方法包括：服务端接收客户端发送的随机数、第一时间戳和第一哈希值；服务端接收客户端发送的加密信息；利用会话密钥对加密信息进行解密得到第一信息和第二信息；将第一信息和第二信息发送到对等网络中。本发明实施例通过客户端将交易信息进行签名，并将交易信息和签名后的信息进行加密，并将加密信息发送给服务端，服务端利用会话密钥对加密信息进行解密得到交易信息，并将交易信息发送到对等网络中，提高了客户端的安全性，使得智能移动终端可以作为区块链节点，并且提高了智能移动终端中个人信息和支付类信息的安全性。



1. 一种区块链节点的实现方法,其特征在于,包括:

服务端接收客户端发送的随机数、第一时间戳和第一哈希值;

所述服务端对所述随机数、所述第一时间戳和预先存储的登陆口令进行哈希运算,得到第二哈希值;

若所述第一哈希值和所述第二哈希值相等,则所述服务端确定所述登陆口令正确;

所述服务端接收客户端发送的加密信息,所述加密信息是所述客户端利用会话密钥对第一信息和第二信息进行加密后得到的信息,所述第一信息包括:交易信息、第二时间戳和第三哈希值,所述第二信息是所述客户端利用区块链节点的私钥对所述第一信息进行签名后得到的信息,所述第三哈希值是对所述交易信息和所述第二时间戳进行哈希运算得到的哈希值;

所述服务端利用所述会话密钥对所述加密信息进行解密得到所述第一信息和所述第二信息;

所述服务端将所述第一信息和所述第二信息发送到对等网络中。

2. 根据权利要求1所述的方法,其特征在于,所述服务端接收客户端发送的加密信息之前,还包括:

所述服务端生成会话密钥,并将所述会话密钥发送给所述客户端。

3. 根据权利要求2所述的方法,其特征在于,所述服务端生成会话密钥,并将所述会话密钥发送给所述客户端,包括:

所述服务端利用所述区块链节点的公钥对所述会话密钥加密,并将加密后的会话密钥发送给所述客户端。

4. 根据权利要求1-3任一项所述的方法,其特征在于,所述服务端接收客户端发送的随机数、第一时间戳和第一哈希值之前,还包括:

所述服务端接收客户端发送的登陆口令和所述区块链节点的公钥。

5. 根据权利要求4所述的方法,其特征在于,还包括:

所述服务端接收客户端发送的账本请求信息;

所述服务端根据所述账本请求信息,将所述服务端存储的账本发送给所述客户端。

6. 一种服务端,其特征在于,包括:

接收模块,用于接收客户端发送的随机数、第一时间戳和第一哈希值;

计算模块,用于对所述随机数、所述第一时间戳和预先存储的登陆口令进行哈希运算,得到第二哈希值;

确定模块,若所述第一哈希值和所述第二哈希值相等,则所述确定模块确定所述登陆口令正确;

所述接收模块还用于接收客户端发送的加密信息,所述加密信息是所述客户端利用会话密钥对第一信息和第二信息进行加密后得到的信息,所述第一信息包括:交易信息、第二时间戳和第三哈希值,所述第二信息是所述客户端利用区块链节点的私钥对所述第一信息进行签名后得到的信息,所述第三哈希值是对所述交易信息和所述第二时间戳进行哈希运算得到的哈希值;

解密模块,用于利用所述会话密钥对所述加密信息进行解密得到所述第一信息和所述第二信息;

发送模块,用于将所述第一信息和所述第二信息发送到对等网络中。

7. 根据权利要求6所述的服务端,其特征在于,还包括:

生成模块,用于生成会话密钥;

所述发送模块还用于将所述会话密钥发送给所述客户端。

8. 根据权利要求7所述的服务端,其特征在于,还包括:

加密模块,用于利用所述区块链节点的公钥对所述会话密钥加密;

所述发送模块具体用于将加密后的会话密钥发送给所述客户端。

9. 根据权利要求6-8任一项所述的服务端,其特征在于,所述接收模块还用于:

接收客户端发送的登陆口令和所述区块链节点的公钥。

10. 根据权利要求9所述的服务端,其特征在于,所述接收模块还用于:接收客户端发送的账本请求信息;

所述发送模块还用于:

根据所述账本请求信息,将所述服务端存储的账本发送给所述客户端。

## 区块链节点的实现方法及装置

### 技术领域

[0001] 本发明实施例涉及通信技术领域，尤其涉及一种区块链节点的实现方法及装置。

### 背景技术

[0002] 区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式。区块链技术是利用块链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算范式。

[0003] 但是，目前用户终端例如智能移动终端无法作为区块链节点，因为，智能移动终端上存储有用户个人信息和支付类信息，如果将智能移动终端作为区块链节点，容易给个人信息和支付类信息造成安全隐患。

### 发明内容

[0004] 本发明实施例提供一种区块链节点的实现方法及装置，以使得智能移动终端可以作为区块链节点，并且提高智能移动终端中个人信息和支付类信息的安全性。

[0005] 本发明实施例的一个方面是提供一种区块链节点的实现方法，包括：

[0006] 服务端接收客户端发送的随机数、第一时间戳和第一哈希值；

[0007] 所述服务端对所述随机数、所述第一时间戳和预先存储的登陆口令进行哈希运算，得到第二哈希值；

[0008] 若所述第一哈希值和所述第二哈希值相等，则所述服务端确定所述登陆口令正确；

[0009] 所述服务端接收客户端发送的加密信息，所述加密信息是所述客户端利用会话密钥对第一信息和第二信息进行加密后得到的信息，所述第一信息包括：交易信息、第二时间戳和第三哈希值，所述第二信息是所述客户端利用区块链节点的私钥对所述第一信息进行签名后得到的信息，所述第三哈希值是对所述交易信息和所述第二时间戳进行哈希运算得到的哈希值；

[0010] 所述服务端利用所述会话密钥对所述加密信息进行解密得到所述第一信息和所述第二信息；

[0011] 所述服务端将所述第一信息和所述第二信息发送到对等网络中。

[0012] 本发明实施例的另一个方面是提供一种服务端，包括：

[0013] 接收模块，用于接收客户端发送的随机数、第一时间戳和第一哈希值；

[0014] 计算模块，用于对所述随机数、所述第一时间戳和预先存储的登陆口令进行哈希运算，得到第二哈希值；

[0015] 确定模块，若所述第一哈希值和所述第二哈希值相等，则所述确定模块确定所述登陆口令正确；

[0016] 所述接收模块还用于接收客户端发送的加密信息，所述加密信息是所述客户端利

用会话密钥对第一信息和第二信息进行加密后得到的信息，所述第一信息包括：交易信息、第二时间戳和第三哈希值，所述第二信息是所述客户端利用区块链节点的私钥对所述第一信息进行签名后得到的信息，所述第三哈希值是对所述交易信息和所述第二时间戳进行哈希运算得到的哈希值；

[0017] 解密模块，用于利用所述会话密钥对所述加密信息进行解密得到所述第一信息和所述第二信息；

[0018] 发送模块，用于将所述第一信息和所述第二信息发送到对等网络中。

[0019] 本发明实施例提供的区块链节点的实现方法及装置，通过客户端将交易信息进行签名，并将交易信息和签名后的信息进行加密，并将加密信息发送给服务端，服务端利用会话密钥对加密信息进行解密得到交易信息，并将交易信息发送到对等网络中，提高了客户端的安全性，使得智能移动终端可以作为区块链节点，并且提高了智能移动终端中个人信息和支付类信息的安全性。

## 附图说明

[0020] 图1为本发明实施例提供的区块链节点的实现方法流程图；

[0021] 图2为本发明另一实施例提供的区块链节点的实现方法流程图；

[0022] 图3为本发明实施例提供的服务端的结构图；

[0023] 图4为本发明另一实施例提供的服务端的结构图。

## 具体实施方式

[0024] 图1为本发明实施例提供的区块链节点的实现方法流程图。本发明实施例提供了区块链节点的实现方法，该方法包括步骤如下：

[0025] 步骤S101、服务端接收客户端发送的随机数、第一时间戳和第一哈希值。

[0026] 在本实施例中，用户设备例如智能移动终端上安装有区块链的客户端，网络侧设备例如服务器上设置有持续在线的服务端，客户端和服务端可以通信。

[0027] 网络侧设备例如服务器进行服务端的初始化，该初始化后，服务端具有如下功能：

[0028] 1) 接入对等网络(Peer to Peer，简称P2P)。

[0029] 2) 进行广播消息的发送接收和处理。

[0030] 3) 记账权的获取计算和抢夺，获取相应的奖励(例如，比特币矿工挖矿的奖励)。

[0031] 4) 存储账本。

[0032] 5) 存储区块链节点的公钥。

[0033] 智能移动终端下载并安装区块链的客户端，安装完毕以后，启动该客户端，生成区块链节点的公钥和私钥。在本实施例中，智能移动终端可以作为一个区块链节点。智能移动终端上安装的区块链的客户端具有如下功能：

[0034] 1) 某个交易的发起和确认。

[0035] 2) 电子合同的签署。

[0036] 3) 存储区块链节点的私钥。

[0037] 智能移动终端的客户端与网络侧设备例如服务器的服务端进行首次互联操作，客户端在服务端上设置初始化登录口令，并同时上传区块链节点的公钥给服务端。服务端收

到登录口令和公钥后，服务端存储该登录口令和公钥，然后回复成功信息给客户端，表示“握手”成功。

[0038] 客户端对登录口令、随机数、第一时间戳进行哈希运算，得到第一哈希值HASH1，然后将随机数、第一时间戳和第一哈希值发送给服务端。

[0039] 步骤S102、所述服务端对所述随机数、所述第一时间戳和预先存储的登陆口令进行哈希运算，得到第二哈希值。

[0040] 服务端对随机数、第一时间戳和第一哈希值进行验证，具体的，对随机数、第一时间戳和预先存储的登陆口令进行哈希运算，得到第二哈希值HASH2。

[0041] 步骤S103、若所述第一哈希值和所述第二哈希值相等，则所述服务端确定所述登陆口令正确。

[0042] 如果HASH1=HASH2，则证明该客户端的登陆口令正确，执行步骤S104，否则，认为该客户端为黑客攻击，记录下对方的MAC地址，以后对于该MAC地址的报文截止做丢弃处理。

[0043] 步骤S104、所述服务端接收客户端发送的加密信息，所述加密信息是所述客户端利用会话密钥对第一信息和第二信息进行加密后得到的信息，所述第一信息包括：交易信息、第二时间戳和第三哈希值，所述第二信息是所述客户端利用区块链节点的私钥对所述第一信息进行签名后得到的信息，所述第三哈希值是对所述交易信息和所述第二时间戳进行哈希运算得到的哈希值。

[0044] 当客户端主动发起某个交易的时候，客户端需要连接到网络中，客户端对该交易的实体内容用区块链节点的私钥进行签名，具体的，利用区块链节点的私钥对交易信息、第二时间戳和第三哈希值进行签名，在本实施例中，将交易信息、第二时间戳和第三哈希值记为第一信息，将利用区块链节点的私钥对交易信息、第二时间戳和第三哈希值进行签名得到的签名信息记为第二信息，其中，所述第三哈希值是对所述交易信息和所述第二时间戳进行哈希运算得到的哈希值。该客户端利用会话密钥对第一信息和第二信息进行加密，得到加密信息，并将该加密信息发送给服务端。

[0045] 步骤S105、所述服务端利用所述会话密钥对所述加密信息进行解密得到所述第一信息和所述第二信息。

[0046] 步骤S106、所述服务端将所述第一信息和所述第二信息发送到对等网络中。

[0047] 服务端接收到加密信息后，利用所述会话密钥对所述加密信息进行解密得到所述第一信息和所述第二信息，即得到交易信息、第二时间戳和第三哈希值，以及利用区块链节点的私钥对交易信息、第二时间戳和第三哈希值进行签名得到的签名信息。服务端将交易信息、第二时间戳和第三哈希值，以及利用区块链节点的私钥对交易信息、第二时间戳和第三哈希值进行签名得到的签名信息发送到P2P网络中，具体可以广播到P2P网络中。

[0048] 另外，当客户端不需要发起交易的时候，客户端和智能移动终端可以保持离线的状态，节约智能移动终端的电池和上网流量，并同时避免了一直在线的状态下容易被黑客攻击等安全问题。

[0049] 服务端一直保持着在线状态，在网络中实时抢夺记账权，以及获取奖励，并存储账本等。

[0050] 本发明实施例通过客户端将交易信息进行签名，并将交易信息和签名后的信息进行加密，并将加密信息发送给服务端，服务端利用会话密钥对加密信息进行解密得到交易

信息，并将交易信息发送到对等网络中，提高了客户端的安全性，使得智能移动终端可以作为区块链节点，并且提高了智能移动终端中个人信息和支付类信息的安全性。

[0051] 图2为本发明另一实施例提供的区块链节点的实现方法流程图。在上述实施例的基础上，本发明实施例提供的区块链节点的实现方法的具体步骤如下：

[0052] 步骤S201、所述服务端接收客户端发送的登陆口令和所述区块链节点的公钥。

[0053] 智能移动终端的客户端与网络侧设备例如服务器的服务端进行首次互联操作，客户端在服务端上设置初始化登录口令，并同时上传区块链节点的公钥给服务端。服务端收到登录口令和公钥后，服务端存储该登录口令和公钥，然后回复成功信息给客户端，表示“握手”成功。

[0054] 步骤S202、服务端接收客户端发送的随机数、第一时间戳和第一哈希值。

[0055] 步骤S202与步骤S101一致，此处不再赘述。

[0056] 步骤S203、所述服务端对所述随机数、所述第一时间戳和预先存储的登陆口令进行哈希运算，得到第二哈希值。

[0057] 步骤S203与步骤S102一致，此处不再赘述。

[0058] 步骤S204、若所述第一哈希值和所述第二哈希值相等，则所述服务端确定所述登陆口令正确。

[0059] 步骤S204与步骤S103一致，此处不再赘述。

[0060] 步骤S205、所述服务端生成会话密钥，并将所述会话密钥发送给所述客户端。

[0061] 具体的，所述服务端利用所述区块链节点的公钥对所述会话密钥加密，并将加密后的会话密钥发送给所述客户端。

[0062] 在本实施例中，引入会话密钥的作用是：防止黑客仿造客户端的IP地址，替代客户端发送假的交易信息给服务端。

[0063] 步骤S206、所述服务端接收客户端发送的加密信息，所述加密信息是所述客户端利用会话密钥对第一信息和第二信息进行加密后得到的信息，所述第一信息包括：交易信息、第二时间戳和第三哈希值，所述第二信息是所述客户端利用区块链节点的私钥对所述第一信息进行签名后得到的信息，所述第三哈希值是对所述交易信息和所述第二时间戳进行哈希运算得到的哈希值。

[0064] 步骤S206与步骤S104一致，此处不再赘述。

[0065] 步骤S207、所述服务端利用所述会话密钥对所述加密信息进行解密得到所述第一信息和所述第二信息。

[0066] 步骤S207与步骤S105一致，此处不再赘述。

[0067] 步骤S208、所述服务端将所述第一信息和所述第二信息发送到对等网络中。

[0068] 步骤S208与步骤S106一致，此处不再赘述。

[0069] 步骤S209、所述服务端接收客户端发送的账本请求信息。

[0070] 步骤S210、所述服务端根据所述账本请求信息，将所述服务端存储的账本发送给所述客户端。

[0071] 可选的，当客户端主动登录服务端并查询账本时，服务端将账本发送给客户端，若客户端不主动登录服务端也不查询账本，则服务端不主动发送账本给客户端。服务端可以执行客户端的网络代理职责。

[0072] 另外,客户端每次发送交易信息,服务端都需要验证一次最初的登陆口令是否正确。也就是说,每次交易信息需要发布时,客户端均需要将该交易信息发送给服务端,服务端需要针对该交易信息生成一个会话密钥,每次的会话密钥不同,避免了海量数据累计后,密钥被人猜测和伪造。

[0073] 图3为本发明实施例提供的服务端的结构图。本发明实施例提供的服务端可以执行区块链节点的实现方法实施例提供的处理流程,如图3所示,服务端30包括:接收模块31、计算模块32、确定模块33、解密模块34、发送模块35;其中,接收模块31用于接收客户端发送的随机数、第一时间戳和第一哈希值;计算模块32用于对所述随机数、所述第一时间戳和预先存储的登陆口令进行哈希运算,得到第二哈希值;若所述第一哈希值和所述第二哈希值相等,则确定模块33确定所述登陆口令正确;接收模块31还用于接收客户端发送的加密信息,所述加密信息是所述客户端利用会话密钥对第一信息和第二信息进行加密后得到的信息,所述第一信息包括:交易信息、第二时间戳和第三哈希值,所述第二信息是所述客户端利用区块链节点的私钥对所述第一信息进行签名后得到的信息,所述第三哈希值是对所述交易信息和所述第二时间戳进行哈希运算得到的哈希值;解密模块34用于利用所述会话密钥对所述加密信息进行解密得到所述第一信息和所述第二信息;发送模块35用于将所述第一信息和所述第二信息发送到对等网络中。

[0074] 本发明实施例提供的服务端可以具体用于执行上述图1所提供的方法实施例,具体功能此处不再赘述。

[0075] 本发明实施例通过客户端将交易信息进行签名,并将交易信息和签名后的信息进行加密,并将加密信息发送给服务端,服务端利用会话密钥对加密信息进行解密得到交易信息,并将交易信息发送到对等网络中,提高了客户端的安全性,使得智能移动终端可以作为区块链节点,并且提高了智能移动终端中个人信息和支付类信息的安全性。

[0076] 图4为本发明另一实施例提供的服务端的结构图。在上述实施例的基础上,服务端30还包括:生成模块36、加密模块37;生成模块36用于生成会话密钥;发送模块35还用于将所述会话密钥发送给所述客户端。

[0077] 加密模块37用于利用所述区块链节点的公钥对所述会话密钥加密;发送模块35具体用于将加密后的会话密钥发送给所述客户端。

[0078] 另外,接收模块31还用于:接收客户端发送的登陆口令和所述区块链节点的公钥。

[0079] 此外,接收模块31还用于:接收客户端发送的账本请求信息;发送模块35还用于:根据所述账本请求信息,将所述服务端存储的账本发送给所述客户端。

[0080] 本发明实施例提供的服务端可以具体用于执行上述图2所提供的方法实施例,具体功能此处不再赘述。

[0081] 本发明实施例通过客户端将交易信息进行签名,并将交易信息和签名后的信息进行加密,并将加密信息发送给服务端,服务端利用会话密钥对加密信息进行解密得到交易信息,并将交易信息发送到对等网络中,提高了客户端的安全性,使得智能移动终端可以作为区块链节点,并且提高了智能移动终端中个人信息和支付类信息的安全性。

[0082] 综上所述,本发明实施例通过客户端将交易信息进行签名,并将交易信息和签名后的信息进行加密,并将加密信息发送给服务端,服务端利用会话密钥对加密信息进行解密得到交易信息,并将交易信息发送到对等网络中,提高了客户端的安全性,使得智能移动

终端可以作为区块链节点，并且提高了智能移动终端中个人信息和支付类信息的安全性。

[0083] 在本发明所提供的几个实施例中，应该理解到，所揭露的装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

[0084] 所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0085] 另外，在本发明各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用硬件加软件功能单元的形式实现。

[0086] 上述以软件功能单元的形式实现的集成的单元，可以存储在一个计算机可读取存储介质中。上述软件功能单元存储在一个存储介质中，包括若干指令用以使得一台计算机设备(可以是个人计算机，服务器，或者网络设备等)或处理器(processor)执行本发明各个实施例所述方法的部分步骤。而前述的存储介质包括：U盘、移动硬盘、只读存储器(Read-Only Memory, ROM)、随机存取存储器(Random Access Memory, RAM)、磁碟或者光盘等各种可以存储程序代码的介质。

[0087] 本领域技术人员可以清楚地了解到，为描述的方便和简洁，仅以上述各功能模块的划分进行举例说明，实际应用中，可以根据需要而将上述功能分配由不同的功能模块完成，即将装置的内部结构划分成不同的功能模块，以完成以上描述的全部或者部分功能。上述描述的装置的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

[0088] 最后应说明的是：以上各实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述各实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分或者全部技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的范围。

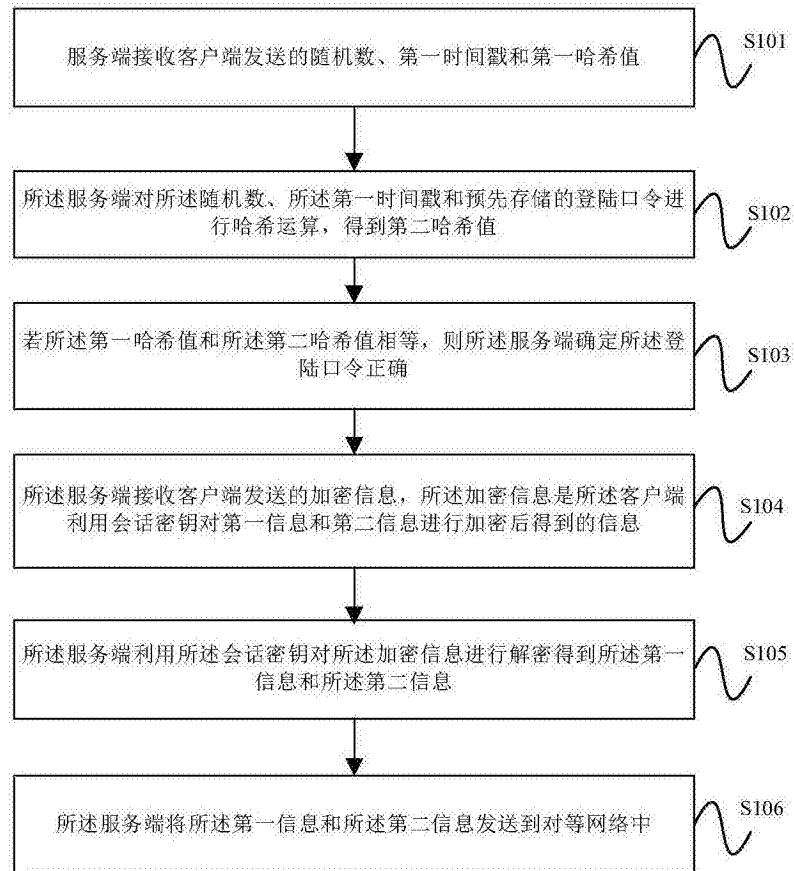


图1

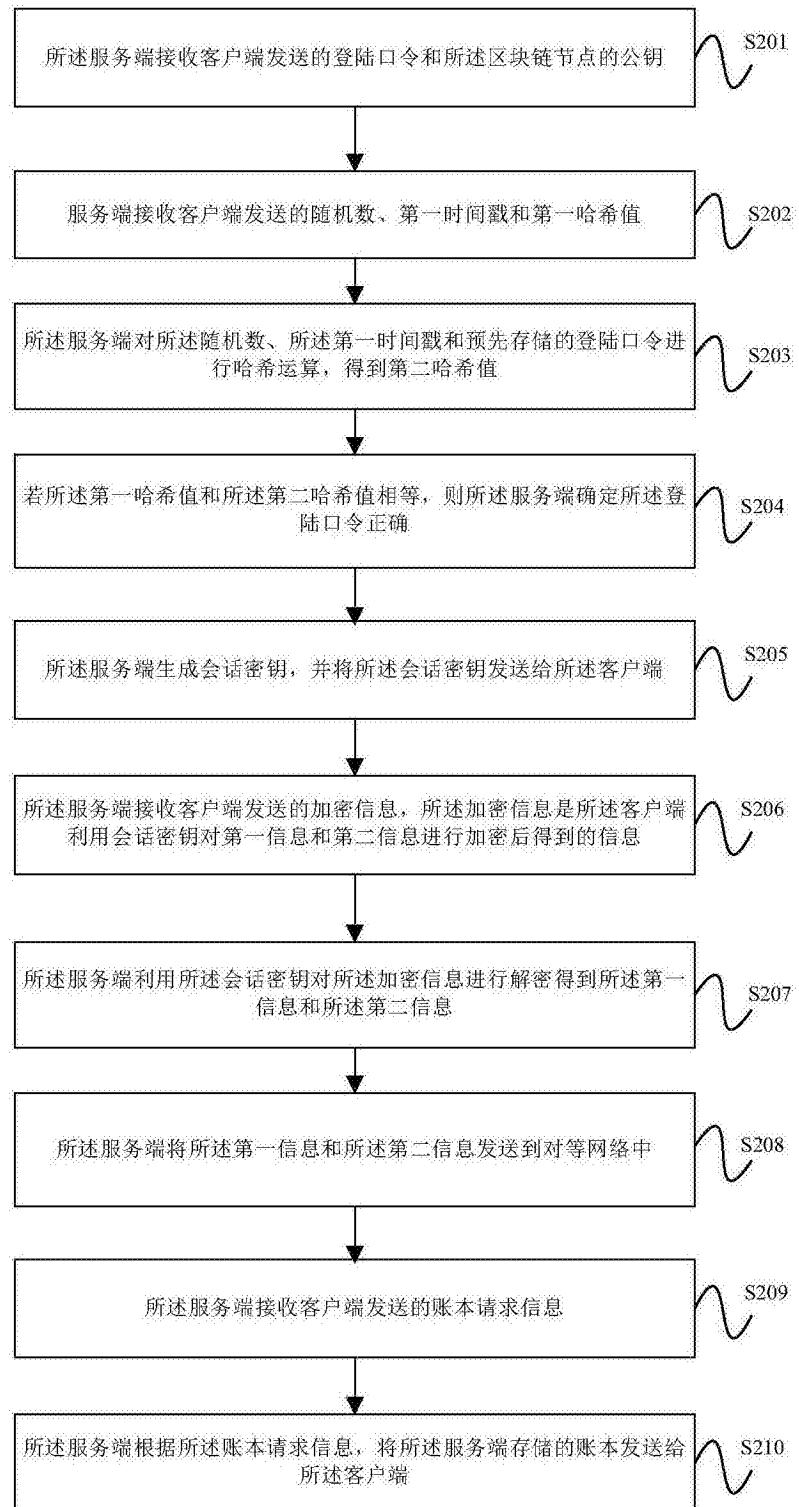


图2

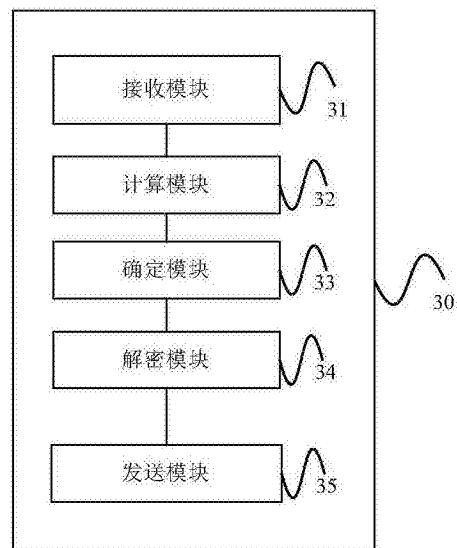


图3

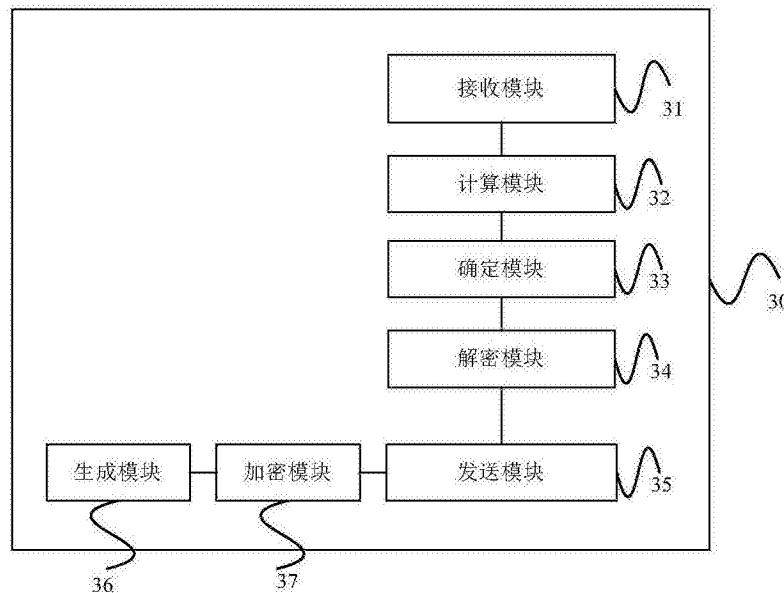


图4