



(12)发明专利申请

(10)申请公布号 CN 107124278 A

(43)申请公布日 2017.09.01

(21)申请号 201710203678.3

(22)申请日 2017.03.30

(71)申请人 腾讯科技(深圳)有限公司

地址 518057 广东省深圳市南山区高新区  
科技中一路腾讯大厦35层

(72)发明人 郭锐 李茂材 赵琦 张建俊  
屠海涛 王宗友 梁军 朱大卫  
陈立生 刘斌华

(74)专利代理机构 北京三高永信知识产权代理  
有限责任公司 11138

代理人 朱雅男

(51)Int.Cl.

H04L 9/32(2006.01)

H04L 9/08(2006.01)

H04L 29/08(2006.01)

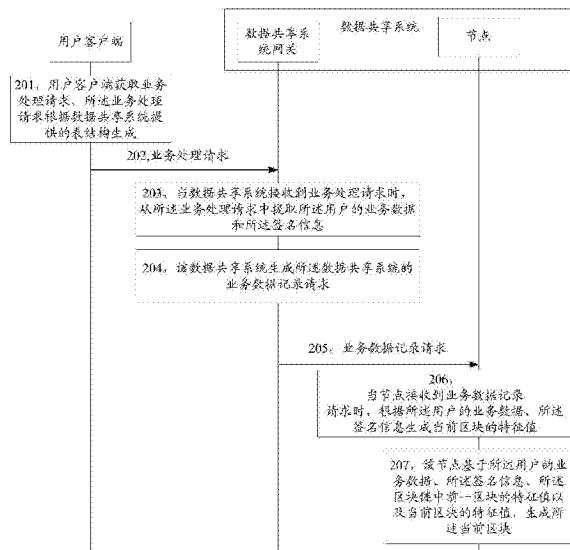
权利要求书4页 说明书18页 附图10页

(54)发明名称

业务处理方法、装置以及数据共享系统

(57)摘要

本发明公开了一种业务处理方法、装置以及数据共享系统，属于网络技术领域。所述方法包括：接收业务处理请求，所述业务处理请求根据数据共享系统提供的表结构生成，所述业务处理请求携带用户的业务数据和所述用户对所述业务数据的签名信息；从所述业务处理请求中提取所述用户的业务数据和所述签名信息；生成所述数据共享系统的业务数据记录请求，所述业务数据记录请求携带所述用户的业务数据以及所述签名信息；将所述业务数据记录请求发送至所述数据共享系统中的至少一个节点。本发明大大降低了数据共享系统的技术门槛，能够多种现有的数据库业务系统均可以与数据共享系统实现无缝对接，提高了区块链技术的普适性。



1.一种业务处理方法,其特征在于,所述方法包括:

接收业务处理请求,所述业务处理请求根据数据共享系统提供的表结构生成,所述业务处理请求携带用户的业务数据和所述用户对所述业务数据的签名信息;

从所述业务处理请求中提取所述用户的业务数据和所述签名信息;

生成所述数据共享系统的业务数据记录请求,所述业务数据记录请求携带所述用户的业务数据以及所述签名信息;

将所述业务数据记录请求发送至所述数据共享系统中的至少一个节点。

2.根据权利要求1所述的方法,其特征在于,所述从所述业务处理请求中提取所述用户的业务数据和所述签名信息包括:

识别生成所述业务处理请求的数据库类型;

根据所述数据库类型,从数据库类型与表结构的对应关系中,确定生成所述业务处理请求所采用的表结构;

基于生成所述业务处理请求所采用的表结构,从所述业务处理请求的对应字段中提取所述用户的业务数据和所述签名信息。

3.根据权利要求1所述的方法,其特征在于,所述接收业务处理请求之前,所述方法还包括:

用户客户端获取所述用户基于所述表结构所输入的业务数据;

所述用户客户端从所述用户客户端中获取所述用户的私钥,并采用所述私钥对所述业务数据进行签名,得到所述用户的签名信息;

将所述业务数据和所述用户的签名信息封装为所述业务处理请求。

4.根据权利要求1所述的方法,其特征在于,所述方法还包括:

当节点接收到所述业务数据记录请求时,将所述用户的业务数据、所述签名信息分为至少两部分数据;对所述至少两部分数据分别采用不同的哈希算法进行计算,得到所述至少两部分数据的哈希值;

将所述至少两部分数据的哈希值拼接,得到所述当前区块的特征值;

基于所述用户的业务数据、所述签名信息、区块链中前一区块的特征值以及当前区块的特征值,生成所述当前区块。

5.根据权利要求1所述的方法,其特征在于,所述基于所述用户的业务数据、所述签名信息、所述区块链中前一区块的特征值以及当前区块的特征值,生成所述当前区块包括:

所述节点采用节点的私钥对所述用户的业务数据、所述签名信息、所述区块链中前一区块的特征值以及当前区块的特征值进行签名,得到所述当前区块的签名信息;

将所述用户的业务数据、所述签名信息、所述区块链中前一区块的特征值、当前区块的特征值以及所述当前区块的签名信息对应存储,生成所述当前区块。

6.一种业务处理方法,其特征在于,所述方法包括:

接收用户客户端的业务处理请求,所述业务处理请求携带业务数据以及所述用户客户端的公钥,所述业务数据包括所述用户客户端的地址信息;

根据所述用户客户端的公钥,生成所述用户客户端的校验地址信息;

如果所述用户客户端的校验地址信息和所述业务数据所包括的地址信息一致,则响应所述业务处理请求,如果不一致,则拦截所述业务处理请求。

7. 根据权利要求6所述的方法,其特征在于,所述根据所述用户客户端的公钥,生成所述用户客户端的校验地址信息包括:

获取所述用户客户端的公钥哈希值;

对所述公钥哈希值进行至少两次哈希运算,得到所述公钥哈希值的哈希值;

从所述公钥哈希值的哈希值中提取前预设位数的字节作为校验码;

将所述公钥哈希值和所述校验码进行拼接,并对拼接得到的字符串进行符合所述数据共享系统所支持的数据格式的编码处理,得到所述用户客户端的地址信息。

8. 根据权利要求7所述的方法,其特征在于,所述将所述公钥哈希值和所述校验码进行拼接包括:

将所述数据共享系统的版本信息、所述公钥哈希值和所述校验码进行拼接。

9. 一种业务处理方法,其特征在于,所述方法包括:

获取业务数据;

获取用户客户端的私钥;

采用所述用户客户端的私钥对所述业务数据进行签名,得到所述用户客户端的签名信息;

根据所述用户客户端的私钥生成所述用户客户端的公钥;

将所述业务数据、所述用户客户端的签名信息和所述用户客户端的公钥封装为业务处理请求,并向数据共享系统发送所述业务处理请求。

10. 根据权利要求9所述的方法,其特征在于,所述获取用户客户端的私钥包括:

采用非对称加密算法,生成第一指定位数的随机数;

将该第一指定位数的随机数进行位数扩展,得到第二指定位数的随机数。

11. 一种业务处理装置,其特征在于,所述装置包括:

接收模块,用于接收业务处理请求,所述业务处理请求根据数据共享系统提供的表结构生成,所述业务处理请求携带用户的业务数据和所述用户对所述业务数据的签名信息;

提取模块,用于从所述业务处理请求中提取所述用户的业务数据和所述签名信息;

生成模块,用于生成所述数据共享系统的业务数据记录请求,所述业务数据记录请求携带所述用户的业务数据以及所述签名信息;

发送模块,用于将所述业务数据记录请求发送至所述数据共享系统中的至少一个节点。

12. 根据权利要求11所述的装置,其特征在于,所述提取模块用于识别生成所述业务处理请求的数据库类型;根据所述数据库类型,从数据库类型与表结构的对应关系中,确定生成所述业务处理请求所采用的表结构;基于生成所述业务处理请求所采用的表结构,从所述业务处理请求的对应字段中提取所述用户的业务数据和所述签名信息。

13. 根据权利要求11所述的装置,其特征在于,所述用户客户端用于获取所述用户基于所述表结构所输入的业务数据;所述用户客户端从所述用户客户端中获取所述用户的私钥,并采用所述私钥对所述业务数据进行签名,得到所述用户的签名信息;将所述业务数据和所述用户的签名信息封装为所述业务处理请求。

14. 根据权利要求11所述的装置,其特征在于,所述数据共享系统的节点包括:

特征值生成模块,用于当节点接收到所述业务数据记录请求时,将所述用户的业务数

据、所述签名信息分为至少两部分数据；对所述至少两部分数据分别采用不同的哈希算法进行计算，得到所述至少两部分数据的哈希值；将所述至少两部分数据的哈希值拼接，得到所述当前区块的特征值；

区块生成模块，用于将所述用户的业务数据、所述签名信息、所述区块链中前一区块的特征值、当前区块的特征值以及所述当前区块的签名信息对应存储，生成所述当前区块。

15. 根据权利要求11所述的装置，其特征在于，所述区块生成模块用于采用节点的私钥对所述用户的业务数据、所述签名信息、所述区块链中前一区块的特征值以及当前区块的特征值进行签名，得到所述当前区块的签名信息；将所述用户的业务数据、所述签名信息、所述区块链中前一区块的特征值、当前区块的特征值以及所述当前区块的签名信息对应存储，生成所述当前区块。

16. 一种业务处理装置，其特征在于，所述装置包括：

接收模块，用于接收用户客户端的业务处理请求，所述业务处理请求携带业务数据以及所述用户客户端的公钥，所述业务数据包括所述用户客户端的地址信息；

生成模块，用于根据所述用户客户端的公钥，生成所述用户客户端的校验地址信息；

业务请求处理模块，用于如果所述用户客户端的校验地址信息和所述业务数据所包括的地址信息一致，则响应所述业务处理请求，如果不一致，则拦截所述业务处理请求。

17. 根据权利要求16所述的装置，其特征在于，所述根生成模块包括：

公钥哈希值获取子模块，用于获取所述用户客户端的公钥哈希值；

哈希值获取子模块，用于对所述公钥哈希值进行至少两次哈希运算，得到所述公钥哈希值的哈希值；

校验码获取子模块，用于从所述公钥哈希值的哈希值中提取前预设位数的字节作为校验码；

地址信息获取子模块，用于将所述公钥哈希值和所述校验码进行拼接，并对拼接得到的字符串进行符合所述数据共享系统所支持的数据格式的编码处理，得到所述用户客户端的地址信息。

18. 一种业务处理装置，其特征在于，所述装置包括：

业务数据获取模块，用于获取业务数据；

私钥获取模块，用于获取用户客户端的私钥；

签名模块，用于采用所述用户客户端的私钥对所述业务数据进行签名，得到所述用户客户端的签名信息；

公钥生成模块，用于根据所述用户客户端的私钥生成所述用户客户端的公钥；

请求发送模块，用于将所述业务数据、所述用户客户端的签名信息和所述用户客户端的公钥封装为业务处理请求，并向数据共享系统发送所述业务处理请求。

19. 根据权利要求18所述的装置，其特征在于，所述私钥获取模块包括：

随机数生成子模块，用于采用非对称加密算法，生成第一指定位数的随机数；

扩展子模块，用于将该第一指定位数的随机数进行位数扩展，得到第二指定位数的随机数。

20. 一种数据共享系统，其特征在于，所述数据共享系统用于为用户客户端提供数据服务，所述数据共享系统包括数据共享系统网关和多个节点；

其中,所述数据共享系统网关用于接收业务处理请求,所述业务处理请求根据数据共享系统提供的表结构生成,所述业务处理请求携带用户的业务数据和所述用户对所述业务数据的签名信息;从所述业务处理请求中提取所述用户的业务数据和所述签名信息;生成所述数据共享系统的业务数据记录请求,所述业务数据记录请求携带所述用户的业务数据以及所述签名信息;将所述业务数据记录请求发送至所述数据共享系统中的至少一个节点;

所述多个节点中的任一个节点用于基于接收到的业务数据记录请求提供数据服务。

## 业务处理方法、装置以及数据共享系统

### 技术领域

[0001] 本发明涉及网络技术领域,特别涉及一种业务处理方法、装置以及数据共享系统。

### 背景技术

[0002] 随着信息技术的不断发展,区块链作为一项全新的技术得到大力的发展。区块链技术脱胎于2008年出现的比特币技术,是比特币的底层技术。区块链是指一串使用密码学方法相关联产生的区块,区块链中每个区块中的区块数据均与上一个区块中的区块数据存在关联,因此,无法通过篡改区块数据来进行作弊,能够确保任何区块上的区块数据均是公开透明的,提高了输入信息的安全性。

[0003] 近年来,由于在安全方面的突出表现,区块链技术经常被应用于例如金融领域的数据服务中。然而,由于区块链技术尤其独特的系统架构以及数据处理方式,很难与传统业务无缝对接,对技术门槛的要求比较高,在适用性上较弱,不利于区块链技术的推广和应用,因此,亟需一种业务处理方法,以提高区块链技术的普适性高。

### 发明内容

[0004] 为了解决现有技术的问题,本发明实施例提供了一种业务处理方法、装置以及数据共享系统。所述技术方案如下:

[0005] 第一方面,提供了一种业务处理方法,所述方法包括:

[0006] 接收业务处理请求,所述业务处理请求根据数据共享系统提供的表结构生成,所述业务处理请求携带用户的业务数据和所述用户对所述业务数据的签名信息;

[0007] 从所述业务处理请求中提取所述用户的业务数据和所述签名信息;

[0008] 生成所述数据共享系统的业务数据记录请求,所述业务数据记录请求携带所述用户的业务数据以及所述签名信息;

[0009] 将所述业务数据记录请求发送至所述数据共享系统中的至少一个节点。

[0010] 在一种可能实现方式中,所述从所述业务处理请求中提取所述用户的业务数据和所述签名信息包括:

[0011] 识别生成所述业务处理请求的数据库类型;

[0012] 根据所述数据库类型,从数据库类型与表结构的对应关系中,确定生成所述业务处理请求所采用的表结构;

[0013] 基于生成所述业务处理请求所采用的表结构,从所述业务处理请求的对应字段中提取所述用户的业务数据和所述签名信息。

[0014] 在一种可能实现方式中,所述接收业务处理请求之前,所述方法还包括:

[0015] 用户客户端获取所述用户基于所述表结构所输入的业务数据;

[0016] 所述用户客户端从所述用户客户端中获取所述用户的私钥,并采用所述私钥对所述业务数据进行签名,得到所述用户的签名信息;

[0017] 将所述业务数据和所述用户的签名信息封装为所述业务处理请求。

- [0018] 在一种可能实现方式中,所述方法还包括:
- [0019] 当节点接收到所述业务数据记录请求时,根据所述用户的业务数据、所述签名信息生成当前区块的特征值;
- [0020] 基于所述用户的业务数据、所述签名信息、区块链中前一区块的特征值以及当前区块的特征值,生成所述当前区块。
- [0021] 在一种可能实现方式中,所述根据所述用户的业务数据、所述签名信息生成当前区块的特征值包括:
  - [0022] 将所述用户的业务数据、所述签名信息分为至少两部分数据;
  - [0023] 对所述至少两部分数据分别采用不同的哈希算法进行计算,得到所述至少两部分数据的哈希值;
  - [0024] 将所述至少两部分数据的哈希值拼接,得到所述当前区块的特征值。
- [0025] 在一种可能实现方式中,所述将所述用户的业务数据、所述签名信息分为至少两部分数据包括:
  - [0026] 根据所述用户的业务数据、所述签名信息的数据量,确定待分割的份数;
  - [0027] 将所述用户的业务数据、所述签名信息分为所确定的份数的数据。
- [0028] 在一种可能实现方式中,所述基于所述用户的业务数据、所述签名信息、所述区块链中前一区块的特征值以及当前区块的特征值,生成所述当前区块包括:
- [0029] 所述节点采用节点的私钥对所述用户的业务数据、所述签名信息、所述区块链中前一区块的特征值以及当前区块的特征值进行签名,得到所述当前区块的签名信息;
- [0030] 将所述用户的业务数据、所述签名信息、所述区块链中前一区块的特征值、当前区块的特征值以及所述当前区块的签名信息对应存储,生成所述当前区块。
- [0031] 在一种可能实现方式中,所述业务数据包括合约数据,所述合约数据包括合约的执行条件参数以及执行参数。
  - [0032] 在一种可能实现方式中,所述合约数据为包括函数名和参数的二进制代码;或,所述合约数据为脚本代码。
- [0033] 在一种可能实现方式中,所述方法还包括:
- [0034] 如果满足所述执行条件参数,基于所述执行参数执行所述合约数据所指示的业务处理。
- [0035] 第二方面,提供了一种业务处理方法,所述方法还包括:
- [0036] 接收用户客户端的业务处理请求,所述业务处理请求携带业务数据以及所述用户客户端的公钥,所述业务数据包括所述用户客户端的地址信息;
- [0037] 根据所述用户客户端的公钥,生成所述用户客户端的校验地址信息;
- [0038] 如果所述用户客户端的校验地址信息和所述业务数据所包括的地址信息一致,则响应所述业务处理请求,如果不一致,则拦截所述业务处理请求。
- [0039] 在一种可能实现方式中,所述根据所述用户客户端的公钥,生成所述用户客户端的校验地址信息包括:
  - [0040] 获取所述用户客户端的公钥哈希值;
  - [0041] 对所述公钥哈希值进行至少两次哈希运算,得到所述公钥哈希值的哈希值;
  - [0042] 从所述公钥哈希值的哈希值中提取前预设位数的字节作为校验码;

- [0043] 将所述公钥哈希值和所述校验码进行拼接，并对拼接得到的字符串进行符合所述数据共享系统所支持的数据格式的编码处理，得到所述用户客户端的地址信息。
- [0044] 在一种可能实现方式中，所述将所述公钥哈希值和所述校验码进行拼接包括：
- [0045] 将所述数据共享系统的版本信息、所述公钥哈希值和所述校验码进行拼接。
- [0046] 在一种可能实现方式中，所述业务处理请求还包括签名信息，所述签名信息由所述用户客户端采用所述用户客户端的私钥对所述业务数据进行签名得到。
- [0047] 第三方面，提供了一种业务处理方法，所述方法包括：
- [0048] 获取业务数据；
- [0049] 获取用户客户端的私钥；
- [0050] 采用所述用户客户端的私钥对所述业务数据进行签名，得到所述用户客户端的签名信息；
- [0051] 根据所述用户客户端的私钥生成所述用户客户端的公钥；
- [0052] 将所述业务数据、所述用户客户端的签名信息和所述用户客户端的公钥封装为业务处理请求，并向数据共享系统发送所述业务处理请求。
- [0053] 在一种可能实现方式中，所述获取用户客户端的私钥包括：
- [0054] 采用非对称加密算法，生成第一指定位数的随机数；
- [0055] 将该第一指定位数的随机数进行位数扩展，得到第二指定位数的随机数。
- [0056] 在一种可能实现方式中，所述将该第一指定位数的随机数进行位数扩展，得到第二指定位数的随机数包括：
- [0057] 将两个该第一指定位数的随机数进行拼接，得到第二指定位数的随机数。
- [0058] 在一种可能实现方式中，所述将两个所述第一指定位数的随机数进行拼接，得到第二指定位数的随机数包括：
- [0059] 将一个所述第一指定位数的随机数的尾部和另一个所述第一指定位数的随机数的头部相连，得到所述第二指定位数的随机数；或，
- [0060] 将一个所述第一指定位数的随机数中预设位数的字符与另一个所述第一指定位数的随机数中所述预设位数的字符插空混合，得到所述第二指定位数的随机数；或，
- [0061] 将一个所述第一指定位数的随机数和另一个所述第一指定位数的随机数的字符打乱，得到所述第二指定位数的随机数。
- [0062] 第四方面，还提供了一种业务处理装置，该业务处理装置包括多个功能模块，用于执行上述第一方面所提供的任一种可能实现方式的具体过程。
- [0063] 第五方面，还提供了一种业务处理装置，该业务处理装置包括多个功能模块，用于执行上述第二方面所提供的任一种可能实现方式的具体过程。
- [0064] 第六方面，还提供了一种业务处理装置，该业务处理装置包括多个功能模块，用于执行上述第三方面所提供的任一种可能实现方式的具体过程。
- [0065] 第七方面，提供了一数据共享系统，所述数据共享系统用于为用户客户端提供数据服务，所述数据共享系统包括数据共享系统网关和多个节点；
- [0066] 其中，所述数据共享系统网关用于接收业务处理请求，所述业务处理请求根据数据共享系统提供的表结构生成，所述业务处理请求携带用户的业务数据和所述用户对所述业务数据的签名信息；从所述业务处理请求中提取所述用户的业务数据和所述签名信息；

生成所述数据共享系统的业务数据记录请求,所述业务数据记录请求携带所述用户的业务数据以及所述签名信息;将所述业务数据记录请求发送至所述数据共享系统中的至少一个节点;

[0067] 所述多个节点中的任一个节点用于基于接收到的业务数据记录请求提供与所述业务数据记录请求服务的数据服务。

[0068] 本发明实施例提供的技术方案带来的有益效果是:

[0069] 通过为客户端提供数据共享系统所支持的表结构,使得客户端能够基于表结构在数据库中触发数据库语句形式的业务处理请求,从而在数据共享系统侧接收到这类数据库语句形式的业务处理请求时,可以实现对业务处理请求的识别和处理,大大降低了数据共享系统的技术门槛,能够多种现有的数据库业务系统均可以与数据共享系统实现无缝对接,提高了区块链技术的普适性。

## 附图说明

[0070] 为了更清楚地说明本发明实施例中的技术方案,下面将对实施例描述中所需要使用的附图作简单地介绍,显而易见地,下面描述中的附图仅仅是本发明的一些实施例,对于本领域普通技术人员来讲,在不付出创造性劳动的前提下,还可以根据这些附图获得其他的附图。

- [0071] 图1是本发明实施例提供的数据共享系统的结构示意图;
- [0072] 图2是本发明实施例提供的一种业务处理方法的流程图;
- [0073] 图3是本发明实施例提供一种用户客户端的界面显示图;
- [0074] 图4是本发明实施例提供的用户客户端以及数据共享系统之间的适配关系图;
- [0075] 图5是本发明实施例提供的一种区块数据内容的示意图;
- [0076] 图6是本发明实施例提供的一种业务处理方法的流程图;
- [0077] 图7是本发明实施例提供的一种企业客户端与数据共享系统之间的数据交互图;
- [0078] 图8是本发明实施例提供的一种地址信息生成方式的示意图;
- [0079] 图9是本发明实施例提供的一种生成原理图;
- [0080] 图10是本发明实施例提供的一种数据共享系统的层示意图;
- [0081] 图11是本发明实施例提供的一种数据共享系统的功能示意图;
- [0082] 图12是本发明实施例提供的一种业务处理装置的结构示意图;
- [0083] 图13是本发明实施例提供的一种业务处理装置的结构示意图;
- [0084] 图14是本发明实施例提供的一种业务处理装置的结构示意图;
- [0085] 图15是本发明实施例提供的一种终端1500的结构框图;
- [0086] 图16是根据一示例性实施例示出的一种业务处理装置1600的框图。

## 具体实施方式

[0087] 为使本发明的目的、技术方案和优点更加清楚,下面将结合附图对本发明实施方式作进一步地详细描述。

[0088] 参见图1所示的数据共享系统,数据共享系统100是指用于进行节点与节点之间数据共享的系统,该数据共享系统可以为用户客户端提供数据服务,所述数据共享系统包括

数据共享系统网关和多个节点；该数据共享系统中可以包括数据共享系统网关101和多个节点102，数据共享系统网关101用于进行请求转换、地址信息校验等功能，多个节点102可以是指数据共享系统中各个企业服务器以及金融机构服务器等。其中，所述数据共享系统网关101用于接收业务处理请求，所述业务处理请求根据数据共享系统提供的表结构生成，所述业务处理请求携带用户的业务数据和所述用户对所述业务数据的签名信息；从所述业务处理请求中提取所述用户的业务数据和所述签名信息；生成所述数据共享系统的业务数据记录请求，所述业务数据记录请求携带所述用户的业务数据以及所述签名信息；将所述业务数据记录请求发送至所述数据共享系统中的至少一个节点；所述多个节点中的任一个节点用于基于接收到的业务数据记录请求提供数据服务，例如写入共享账本或是账户信息查询等服务。

[0089] 每个节点102在进行正常工作可以接收到用户客户端的输入信息(如业务数据)，并基于接收到的输入信息维护该数据共享系统内的共享数据。为了保证数据共享系统内的信息互通，数据共享系统中的每个节点之间可以采用任一种通信协议，以使得节点之间可以进行信息传输。该通信协议可以包括P2P(Peer to Peer,点对点)、TCP(Transmission Control Protocol传输控制协议)、UDP(User Datagram Protocol,用户数据报协议)以及多播形式。当数据共享系统中的任意节点接收到输入信息时，数据共享系统中的其他节点便根据共识算法获取该输入信息，将该输入信息作为共享数据中的数据进行存储，使得数据共享系统中全部节点上存储的数据均一致。其中，数据共享系统可为交易系统，交易系统指用于金融交易的系统。交易系统中可以包括多个节点，每个节点在进行交易时生成账本数据，并基于账本数据维护该交易系统内的共享账本。

[0090] 现有数据共享系统，还存在一定的缺陷，例如：

[0091] 1、由于区块链技术尤其独特的系统架构以及数据处理方式，很难与传统业务无缝对接，传统的数据库业务，对技术门槛的要求比较高，在适用性上较弱，不利于区块链技术的推广和应用。

[0092] 2、现有的数据共享系统一般采用的密钥强度较低，例如，bitcoin(比特币系统)采用单纯256bits的随机数，单纯采用SHA256摘要算法，将来有可能存在被破解可逆的风险。

[0093] 3、智能合约的安全性与灵活性不兼备。现有的智能合约技术存在很多安全问题，而比特币机制所提供的图灵不完备，其语言不具备多种业务场景使用的灵活性。

[0094] 针对上述缺陷，本发明实施例提供了相应解决方式，下面基于不同侧面对相应解决方式进行介绍。

[0095] 本发明实施例提供了一种业务处理方法，用以降低数据共享系统的技术门槛，能够多种现有的数据库业务系统均可以与数据共享系统实现无缝对接，提高了区块链技术的普适性，参见图2，以用户客户端以及数据共享系统为交互主体为例对该业务处理方法进行说明：

[0096] 在步骤201中，用户客户端获取业务处理请求，该业务处理请求根据数据共享系统提供的表结构生成，该业务处理请求携带用户的业务数据和该用户对该业务数据的签名信息。

[0097] 用户客户端为事先已经注册于数据共享系统的用户所使用的客户端，用户可以通过该用户客户端与数据共享系统进行业务处理。对于该用户客户端来说，在为用户呈现业

务处理界面时,可以在业务处理界面中显示由数据共享系统提供的表结构,使得用户客户端能够基于该表结构获取业务处理请求。其中,表结构是指数据库中的表的名称、具有哪些字段以及哪些字段是主键等用于进行数据查询和数据插入等业务处理时的主要信息。

[0098] 需要说明的是,该构造业务处理请求的过程可以是由用户直接按照表结构输入业务处理请求的数据库语句并由用户客户端向语句中添加签名信息,也可以是由用户客户端基于用户所输入的业务数据等来生成语句,并向语句中添加业务数据的签名信息。其具体过程可以包括:用户客户端获取该用户的业务数据;该用户客户端从用户客户端中获取该用户的私钥,并采用该私钥对该业务数据进行签名,得到该用户的签名信息;将该业务数据和该用户的签名信息封装为该业务处理请求。其中,用户所输入的业务数据后续会被存储于数据共享系统所生成区块的信息字段内。其中,业务数据可以是指用户的交易信息,例如,该业务数据可以包括转出方地址信息,转入方地址信息以及交易金额。

[0099] 另一点需要说明的是,用户客户端在进行签名时,可以基于不同业务处理请求所对应的业务类型,来选择业务数据中的不同长度的数据进行签名,例如,有些业务处理请求的数据库语句本身较长,则可以获取较短的一段业务数据进行签名,而一些业务处理请求的数据库语句本身较短,则可以获取较长的一段业务数据进行签名,从而做到针对不同业务级别的签名。对普通SQL语句自动做业务级别签名。

[0100] 例如,以用户客户端所使用的数据库系统为mysql,而数据共享系统被命名为trustsql为例,trustsql网关(即接入层(API))适配mysql,开发人员可以通过mysql自带驱动连接trustsql以加入该数据共享系统,对于开发人员来说,其所进行的操作与平时操作mysql并无区别,trustsql底层的协议对该用户客户端来说不可见,trustsql为该用户客户端提供固定的表结构可支持在数据共享系统的区块的info字段进行insert、select账户等操作。

[0101] 用户客户端所获取到的sql语句可以为:

[0102] Insert into t\_transaction set//该语句的功能在于向共享账本中加入交易信息

[0103] from\_address='1H3ktZnx6XtxkC4Ck31r4GzjpjWaLHvGVj',//转出方地址信息

[0104] to\_address="1MZLjFBPgXTgWSxZJEhFkgwaTf93cStDCA",//转入方地址信息

[0105] amount=100,//交易金额为100

[0106] sign='MEQCIH0ksbcX9kT0gJ0JkIe2H10DcgHetqA1cf7dMZXapDjAiB9T6e1Q8McMQAvYYbNdWuQrva016/o07YEgqR5jGBy5g',//交易信息的签名

[0107] publickey='BHSgdFFuE8p0FQ5+Ge1A05XAj8su5B8UpAtWo9zNXifUk9+6T4L5rVxhxRWU7t83zek7EYTYap6EY1LW12Qc/Ro';//交易信息的公钥

[0108] 其中,sign是根据椭圆曲线签名算法算出;

[0109] sign=ECDSA(private\_key,(from\_address+to\_address+amount)),

[0110] 其中,private\_key为用户持有的私钥,“from\_address+to\_address+amount”为交易信息,由于私钥是由用户客户端生成以及保存,因此,该签名信息可以防止用户的业务数据被篡改。该私钥的具体生成过程可以参见下述密钥管理部分的详述。

[0111] 如果发生黑客登录数据库篡改,数据共享系统可以基于查询请求中所携带的签名信息与相应区块中所存储的签名信息进行比较,一旦查询确定两次签名信息不一致,则说

明数据被篡改过，并可以通过区块特征值来确定是哪部分业务数据被篡改，从而将该篡改以错误码形式返回给使用者。

[0112] 需要说明的是，对于用户客户端来说，在与数据共享系统适配后，可以屏蔽其他业务表，只暴露该数据共享系统中的区块链表。例如，以用户客户端所使用的数据库系统为mysql为例，在登录用户客户端后，其mysql的显示界面可以从原有表的显示（如图3中上图所示）更改为区块链表（如图3中下图所示）。

[0113] 在步骤202中，该用户客户端向数据共享系统发送该业务处理请求。

[0114] 用户客户端可以通过与数据共享系统之间的连接向数据共享系统发送该业务请求，该发送可以基于事先的系统适配来实现，使得用户客户端可以通过客户端的数据库驱动来向该数据共享系统发送业务处理请求。

[0115] 在步骤203中，当数据共享系统接收到业务处理请求时，从该业务处理请求中提取该用户的业务数据和该签名信息。

[0116] 在本发明实施例中，该数据共享系统可以具有数据共享系统网关，用于隔离外部网络和系统内部的节点，使得对于外部网络用户来说，系统内部的节点对于他们并不透明，不会被外部网络用户感知，至于具体采用什么数据协议也无需被外部网络用户所获知。而数据共享系统网关可以用于接收该业务处理请求，并进行将业务处理请求转换为业务数据记录请求的步骤。

[0117] 由于事先已经做过了用户客户端与数据共享系统之间的适配，因此，数据共享系统的网关可以在接收到业务处理请求后，将业务处理请求中的关键数据提取出来。当然，由于数据共享系统可以支持多个不同的数据库类型，则该步骤203也可以包括下述过程：识别生成该业务处理请求的数据库类型；根据该数据库类型，从数据库类型与表结构的对应关系中，确定生成该业务处理请求所采用的表结构；基于生成该业务处理请求所采用的表结构，从该业务处理请求的对应字段中提取该用户的业务数据和该签名信息。由于不同数据库类型所对应的数据库语句可能有所差别，因此，可以为其提供不同的表结构来生成业务处理请求，因此，在提取过程中也要先识别出到底是由哪种数据库类型生成的业务处理请求，才能做到准确的提取。当然，对于不同的数据库类型，还可以提供相同的表结构，但是仍需知道表结构在不同数据库类型中的含义，也即是获知生成业务处理请求的数据库类型，以实现有效的识别。如图4所示，数据共享系统所支持的数据库类型包括：Oracle、MySQL、SQL server、Redis、memcached以及File等数据库类型，本发明实施例对此不作具体限定。

[0118] 由于在数据共享系统中，一旦增加了支持哪个数据库类型的用户系统，则可以直接在数据共享系统中与数据库协议进行适配，也即是在数据共享系统网关上设置针对该数据库类型的表结构以及提取方式，而无需修改数据共享系统内部已有的数据协议等，而对于用户系统侧来说，由于无需在用户系统侧和数据共享系统内部隔离，用户系统侧只需获知数据共享系统提供的表结构，即可以基于该表结构通过自身已有的数据库驱动来生成业务处理请求，以在数据共享系统中进行共享账本的写入(insert)、选择(select)账户进行操作等。

[0119] 以上述sql语句为例，可以提取出：

[0120] Insert into t\_transaction set

[0121] from\_address = '1H3ktZnx6XtxkC4Ck31r4GzjpjWaLHvGVj' ,

[0122] to\_address = "1MZLjFBPgXTgWSxZJEhFkgwaTf93cStDCA",  
[0123] amount = 100, //以上为业务数据  
[0124] sign = 'MEQCIH0ksbcX9kT0gJ0JkIe2H10DcgHetqA1cfx7dMZXapDjAiB9T6e1Q8McMQ  
AvYYbNdWuQrv016/o07YEgqR5jGBy5g', //签名信息  
[0125] publickey = 'BHSgdFFuE8p0FQ5+Ge1A05XAj8su5B8UpAtWo9zNXifUk9+  
6T4L5rVxhxRWU7t83zek7EYTYap6EY1LW12Qc/Ro'; //公钥

[0126] 进一步地,当数据共享系统接收到业务处理请求时,可以根据业务处理请求所携带的用户客户端的公钥,生成该用户客户端的校验地址信息;如果该用户客户端的校验地址信息和该业务数据所包括的地址信息一致,则响应该业务处理请求,执行步骤203以及后续步骤,如果不一致,则拦截该业务处理请求,不再执行后续步骤,进一步地,还可以提醒用户客户端当前业务处理请求遭到篡改。其中具体生成用户客户端的校验地址信息的过程在后续密钥管理部分进行详述,在这里不做赘述。

[0127] 在步骤204中,该数据共享系统生成该数据共享系统的业务数据记录请求,该业务数据记录请求携带该用户的业务数据以及该签名信息。

[0128] 数据共享系统基于上述提取得到的用户的业务数据以及该签名信息,按照数据共享系统所支持的请求格式,重新生成一条业务数据记录请求,以便在数据共享系统内部实现数据处理。该过程可以看做是对业务处理请求的格式转化,以便使得数据库语句能够被数据共享系统所识别并进行处理。通过这种格式转化,使得数据共享系统的适用性大大增强,降低了技术门槛。

[0129] 在步骤205中,该数据共享系统将该业务数据记录请求发送至该数据共享系统中的至少一个节点。

[0130] 该业务数据记录请求可以在数据共享系统中进行全局发送,也即是,由数据共享系统网关将该业务数据记录请求广播至数据共享系统中的各个节点,也可以由数据共享系统网关将该区块链接入请求广播至数据共享系统的关键节点或是交易节点,而不是全部节点,再由这些节点进行进一步广播,本发明实施例对具体发送至哪些节点不做限定。

[0131] 在步骤206中,当节点接收到该业务数据记录请求时,根据该用户的业务数据、该签名信息生成当前区块的特征值。

[0132] 当节点接收到业务数据记录请求时,则可以获取父区块的区块特征值,父区块为与当前区块相关联的上一个区块,区块链中的每个区块的区块数据均包括输入信息(也即是业务数据)、签名信息、父区块的区块头特征值、输入信息特征值、版本号、时间戳和难度值等。在生成区块时,需要根据上述信息进行特征值计算,计算当前区块的区块特征值。

[0133] 而为了增加破解的难度,在生成当前区块的特征值时,可以采用多种哈希算法进行并联计算,例如,可以将该用户的业务数据、该签名信息等用于生成特征值的信息分为至少两部分数据;对该至少两部分数据分别采用不同的哈希算法进行计算,得到该至少两部分数据的哈希值;将该至少两部分数据的哈希值拼接,得到该当前区块的特征值。例如,该不同的哈希算法可以包括SHA256算法、SM3算法等。

[0134] 其中,该将该用户的业务数据、该签名信息分为至少两部分数据包括:根据该用户的业务数据、该签名信息的数据量,确定待分割的份数;将该用户的业务数据、该签名信息分为所确定的份数的数据。可选地,可以将用于生成特征值的信息均分为两部分,例如

256bits的数据分割为2份,前128bits采用SHA256算法,后128bits采用SM3算法。当然也可以采用三种不同算法,也即是,将用于生成特征值的信息均分为三部分,不同部分采用不同算法,或者相邻部分采用不同算法,本发明实施例对此不做具体限定。并联算法后的特征值更具不可逆性,大大提高了安全性。且还可以根据数据共享系统的算法设置,随时变更生成特征值所采用的算法,以在被破解的情况下,及时起到救济的作用。

[0135] 在步骤207中,该节点基于该用户的业务数据、该签名信息、该区块链中前一区块的特征值以及当前区块的特征值,生成该当前区块。

[0136] 需要说明的是,上述校验通过可以是指数据共享系统中的多个节点采用共识算法确定可以将本次业务数据加入区块链,其具体算法在此处不做介绍,任一种能够实现上述目的从而解决拜占庭问题的算法均可以在此处采用。

[0137] 进一步地,在步骤207的基础上,还可以由节点基于节点自身的私钥对区块内待存储的信息进行再次签名,以达到在业务数据的签名信息的一层防篡改的基础上,第二层防篡改的机制,能够大大提高安全性。也即是,该步骤207可以包括:该节点采用节点的私钥对该用户的业务数据、该签名信息、该区块链中前一区块的特征值以及当前区块的特征值进行签名,得到该当前区块的签名信息;将该用户的业务数据、该签名信息、该区块链中前一区块的特征值、当前区块的特征值以及该当前区块的签名信息对应存储,生成该当前区块。参见图5图中的Node\_sign即是指当前区块的签名信息。Node\_sign由于记录了该节点使用自己的私钥签名本条数据的摘要,可以防止节点被攻破后篡改本地数据。图5中的Index属性标识了每条业务数据的顺序,从1开始,依次递增,如果出现问题节点(也即是区块内的数据出现错误的节点),可按照index编号重新获取其他节点的正确数据修复自己,新加入节点同样可以按照某个index上做的快照,拉取最近的快照数据,与增量的记录,来最快速度追上现有节点的数据。而pre-hash是指父区块的区块特征值,hash是指当前区块的区块特征值。

[0138] 针对现有的数据共享系统的密钥强度较低的问题,本发明实施例提供了一种管理服务,其中包括密钥管理方法,可以通过可扩展的密钥位数和/或可扩展的多种高强度哈希算法并联,以避免由于单一算法而被破解的风险。该密钥管理方法可以是针对数据共享系统的用户。用户是指通过数据共享系统进行业务处理的用户,可以为个人用户或企业用户。为了便于描述,在下文中将这类用户所使用的客户端称为用户客户端,为了能够使用数据共享系统所提供的服务,用户客户端需要在数据共享系统中进行注册,参见图6,下述步骤601至610为该注册过程以及注册成功后的业务处理过程。

[0139] 在步骤601中,用户客户端向数据共享系统发送注册请求。

[0140] 该注册请求可以用于注册数据共享系统,以进行业务处理。作为个人用户的用户客户端可以通过提供个人身份信息等基础信息,即可以进行注册行为。

[0141] 在步骤602中,数据共享系统在接收到该注册请求时,为用户客户端进行注册,并在注册成功时为用户客户端提供密钥生成工具。

[0142] 其中,该密钥生成工具用于指示在用户客户端生成密钥时采用的算法,例如在生成私钥时所采用的算法、在生成公钥时所采用的算法以及在生成地址信息时所采用的算法。

[0143] 另外,对于一般用户来说,其注册请求可以仅携带一些注册必要信息,例如个人身

份信息等,而对于企业用户来说,为了在提交注册请求时,还需提交相应的企业身份信息等资料,以便数据共享系统对其信息进行审核,在审核通过时,才能够对其进行注册。例如,以图7为例,由企业提交资料进行注册,经过审核后,向企业客户端返回密钥生成工具,而在企业客户端基于该密钥生成工具生成了公钥和地址信息后,数据共享系统的密钥管理服务可以记录企业的公钥、地址信息与企业身份的对应信息。公钥是可以公开的,每条业务处理请求可以携带企业客户端的签名信息和公钥,以便标识一个人的身份。另外,企业客户端可以进行基于公钥的账户信息查询,由数据共享系统根据公钥查询该企业客户端所有对应的地址信息,并获取各个地址信息以返回账户信息。该账户信息实际上是指该企业客户端的地址信息所对应的账户余额等信息。当然,还可以基于公钥进行其他业务处理请求,本发明实施例对此不做具体限定。

[0144] 在步骤603中,用户客户端基于密钥生成工具,生成用户客户端的私钥。

[0145] 对于用户客户端来说,其私钥由该用户客户端基于数据共享系统的密钥生成工具自行生成,例如,采用非对称加密算法,生成第一指定位数的随机数;将该第一指定位数的随机数进行位数扩展,得到第二指定位数的随机数,将该第二指定位数的随机数作为该用户客户端的私钥。其中,该位数扩展可以是成整数倍的扩展,如将256bits的随机数扩展为512bits的随机数。具体的位数扩展方式可以是基于该已获取到的随机数本身的字符进行,例如,将两个该第一指定位数的随机数进行拼接,得到第二指定位数的随机数。在这里,主要介绍三种拼接方式:

[0146] (1) 将一个该第一指定位数的随机数的尾部和另一个该第一指定位数的随机数的头部相连,得到该第二指定位数的随机数。

[0147] 这种收尾拼接的方式,使得同一个随机数重复了两次,这种拼接方式较简单,计算量小,可以避免对计算资源的过度占用。例如,对于随机数abc来说,可以将其扩展为abcabc。

[0148] (2) 将一个该第一指定位数的随机数中预设位数的字符与另一个该第一指定位数的随机数中该预设位数的字符插空混合,得到该第二指定位数的随机数。

[0149] 这种插空混合实际上是对随机数进行错位交叉,这种拼接方式也较为简单,计算量小,仅需将其中一个随机数向后错位并与另一个随机数合并即可。例如,对于随机数abcde来说,可以将一个abcde向后错两位,如下述形式:

[0150] abcde

[0151] abcde

[0152] 通过对上述错位后的随机数进行插空混合后,得到abcdbece。

[0153] (3) 将一个该第一指定位数的随机数和另一个该第一指定位数的随机数的字符打乱,得到该第二指定位数的随机数。这种随机打乱的方式由于是随机进行的,因此,其不可逆性最为稳定,使得基于这种私钥所生成的公钥的安全性更高。

[0154] 通过上述位数扩展所得到的私钥,以初始采用算法所生成的随机数为256bits的算法强度为例,如果所设计的可扩展的密钥长度,最大支持到512bits,则按照目前的量子计算机计算速度,假设某超级计算机1秒能暴力尝试10亿个密码,破解15位需要243亿年,破解难度足够保证密钥的安全性。当然,除了上述介绍的几种拼接方式以外,还可以有其他拼接方式,这里不做过多赘述,需知只要能将数字打混的拼接方式均适用于本发明中。

[0155] 在步骤604中,该用户客户端基于用户客户端的私钥和密钥生成工具,生成该用户客户端的公钥,并将该用户客户端的公钥发送至数据共享系统。

[0156] 其中,生成该用户客户端的公钥包括:根据该用户客户端的私钥和密钥生成工具所指示的用于生成公钥的算法,生成该用户客户端的公钥。例如,如果密钥生成工具所指示的用于生成公钥的算法为哈希运算,则可以根据该哈希运算的具体算法对私钥进行计算,以得到公钥。例如,如果该哈希运算的具体算法为SEC0256K1(椭圆曲线算法),则基于该算法得到用户客户端的公钥。

[0157] 在数据共享系统中,可以采用用户客户端的公钥来代表用户客户端的身份,因此,还可以将该公钥发送至数据共享系统,使其基于多个用户客户端的公钥生成公钥列表,并广播至各个节点,以使得各个节点能够在进行业务处理时对业务处理请求进行校验,当接收到任一业务处理请求时,先查询该公钥列表中是否包括该业务处理请求所携带的公钥,如果包括,则可以对该业务处理请求进行下一步处理,例如对签名信息的校验等等。

[0158] 在步骤605中,该用户客户端获取业务数据,并获取用户客户端的私钥。

[0159] 该获取业务数据和私钥的过程与上述步骤201中所描述的过程同理,在此不做赘述。

[0160] 在步骤606中,该用户客户端采用该用户客户端的私钥对该业务数据进行签名,得到该用户客户端的签名信息。

[0161] 该得到签名信息的具体过程也可以与步骤201中的签名信息生成过程同理,在此不做赘述。

[0162] 在步骤607中,该用户客户端根据该用户客户端的私钥生成该用户客户端的公钥。

[0163] 该步骤607是指实时生成公钥的过程,在实际实现中,该公钥也可以是事先生成并存储于用户客户端,以供在有业务需求时从存储器中提取并使用,而无需实时生成,以降低实际运行中所需的计算资源。

[0164] 在步骤608中,该用户客户端将该业务数据、该用户客户端的签名信息和该用户客户端的公钥封装为业务处理请求,并向数据共享系统发送该业务处理请求。

[0165] 该步骤608的过程与步骤201中的业务处理请求生成过程同理,在此不做赘述。

[0166] 在步骤609中,该数据共享系统在接收用户客户端的业务处理请求后,根据该用户客户端的公钥,生成该用户客户端的校验地址信息,该业务处理请求携带业务数据以及该用户客户端的公钥,该业务数据包括该用户客户端的地址信息。

[0167] 其中,根据该用户客户端的公钥,生成该用户客户端的校验地址信息的具体过程可以包括:获取该用户客户端的公钥哈希值;对该公钥哈希值进行至少两次哈希运算,得到该公钥哈希值的哈希值;从该公钥哈希值的哈希值中提取前预设位数的字节作为校验码;将该公钥哈希值和该校验码进行拼接,并对拼接得到的字符串进行符合该数据共享系统所支持的数据格式的编码处理,得到该用户客户端的地址信息。进一步地,在拼接时,还可以加入用于表示系统版本的版本信息,也即是,将该数据共享系统的版本信息、该公钥哈希值和该校验码进行拼接。

[0168] 例如,参见图8,该公钥的生成过程包括:用户客户端基于随机数算法(random(256) bits)生成私钥,再对该私钥进行SEC0256K1运算,以得到公钥,数据共享系统基于公钥采用SHA256进行一次哈希运算,再基于得到的哈希值再次基于RIPEMD160进行一次哈希

运算,得到公钥哈希值,再对公钥哈希值采用国密SM3进行两次哈希运算,以得到一个用于校验的字符串,并获取该字符串的前四位为校验码,进而将版本信息、公钥哈希值以及校验码进行拼接,再将拼接得到的字符串进行BASE58算法运算,以得到用户客户端的地址信息。

[0169] 参见图9可知,地址信息的生成实际上是通过私钥—公钥—公钥哈希值—地址信息这个流向进行,在该生成过程中,经历了多次不可逆运算,并且通过多次不可逆运算大大降低了最终地址信息的数据长度,进而进一步增加了地址信息的不可逆性,使得无法基于地址信息倒推出公钥,也即无法倒推出用户客户端的私钥,由于私钥是进行业务处理的必要信息,因此保障了用户的财产安全。

[0170] 该地址信息事实上就代表了该用户客户端在数据共享系统中的账号,用户客户端可以通过该地址信息与其他用户客户端或是服务器进行业务处理,例如转账、认购等等交易行为。当然,为了进一步提高安全性,还可以在上述步骤中采用算法插拔设计,可在必要的场景切换为国密体系,例如,参见图8,生成私钥时可以将当前采用的SEKO256K1(椭圆曲线算法)替换成国密SM2算法,在对公钥进行哈希运算时可以将当前采用的SHA256算法替换成国密SM3算法,而在生成校验码的时候,可以将当前采用的SHA256算法替换成国密SM3算法。

[0171] 在步骤610中,如果该用户客户端的校验地址信息和该业务数据所包括的地址信息一致,则响应该业务处理请求,如果不一致,则拦截该业务处理请求。

[0172] 在此具体如何对业务处理请求进行响应的过程在此不做赘述,具体可以参照上述图2所示实施例中的节点侧处理过程。

[0173] 而针对智能合约的安全性与灵活性问题,本发明实施例的业务处理请求中所携带的业务数据可以包括合约数据,所述合约数据包括合约的执行条件参数以及执行参数。其中,合约的执行条件参数是指要执行该合约需要满足哪些条件,例如合约到期或是付款已到账等。而对于私有链和联盟链来说,由于存在不同的问题,例如,在完全受控的私有链里,通过在业务数据里直接植入函数名和参数的二进制代码,以形成合约调用,当调用方把智能合约流水写入链上时,其他节点会同步二进制代码,最后基于执行结果一起做共识,来完成一次智能合约调用。在不完全受控的联盟链里,通过在业务数据里植入编写好的脚本代码,以堆栈语言执行的规则执行非图灵完备的脚本代码,通过限制脚本长度做到防止死循环。如果满足所述执行条件参数,基于所述执行参数执行所述合约数据所指示的业务处理。

[0174] 例如,如果你从网上买了某物,你可能不想立即付款,想等到卖家发货后再付款。所以你可以很容易地创建一个智能合约,并将智能合约的相关数据承载在业务处理请求中发至数据共享系统,使得数据共享系统能够将该智能合约加入区块链,而智能合约的内容是只要联邦快递的数据表示商品已经发往目的地址,即将货款转给卖家。则当检测到符合上述条件,即可执行将货款转给卖家的业务处理。

[0175] 本发明实施例所提供的数据共享系统,数据共享系统中可以包括接入层适配插件,该接入层适配插件实际上可以用于进行业务处理请求的格式转换,以使得该数据共享系统能够适用于采用不同数据库协议的客户端,而业务处理请求在经过接入层适配插件的处理后,可以由业务逻辑层进一步处理,例如发送至各个节点、进行身份校验以及其他处理,该处理过程涉及到存储插件、共识插件,还需要基于一定的通信协议进行,对于数据共享系统来说,其底层存储可以基于DB(Data Base,数据库)、文件(File)以及键值KV(Key-

Value) 等进行,而其共识插件主要用于验证数据共享系统内节点上数据的一致性使用,其可以采用Raft、Paxcos以及Pbft等任一种共识算法,而在数据共享系统中,还支持多种通信协议,如P2P、TCP以及广播等等,以实现系统内的数据交互。基于这样的数据共享系统的层架构,上述三个部分从功能上的架构还可以如图11所示,管理服务、数据服务以及智能合约服务。其中,管理服务可以提供密钥相关的管理服务,该管理服务分为密钥管理、身份识别以及节点管理。其中,密钥管理可以基于加强的密钥算法等来实现。节点管理,也即是对于每个需加入、退出联盟链、私有链的节点,在节点管理服务里都可对其进行操作,当新加入节点审批通过时,该节点在联盟链、私有链里会具备身份信息,同时广播到其他节点,每个节点有自己的公私钥对,可对自己节点广播数据做签名,其他节点收到请求后,会对签名的数据做校验,拦截非法信息,防止被篡改的可能。当旧节点需退出联盟链、私有链时,对该节点密钥进行作废处理,同时通知其他各节点,一起作废。而身份识别主要是基于公钥进行,一个公钥可以代表一个用户客户端的身份,用以进行业务处理请求校验、查询校验等等。进一步地,关于数据服务部分,该数据共享服务的数据服务可以基于用户数据进行区块链的相关处理。而智能合约服务主要采用以太坊虚拟机(EVM)是以太坊中智能合约的运行环境。智能合约的代码不仅被沙箱封装起来,事实上它的运行也被完全隔离,也就是说运行在虚拟机中,由于运行于虚拟机内部的代码不能接触到网络、文件系统或者其它进程,因此达到了最大化的安全保障,且智能合约服务能够为用户提供更加多样化和更具有保障性的交易服务,大大扩展了数据共享系统的灵活性。

[0176] 图12是本发明实施例提供的一种业务处理装置的结构示意图。参见图12,所述装置包括:

[0177] 接收模块1201,用于接收业务处理请求,所述业务处理请求根据数据共享系统提供的表结构生成,所述业务处理请求携带用户的业务数据和所述用户对所述业务数据的签名信息;

[0178] 提取模块1202,用于从所述业务处理请求中提取所述用户的业务数据和所述签名信息;

[0179] 生成模块1203,用于生成所述数据共享系统的业务数据记录请求,所述业务数据记录请求携带所述用户的业务数据以及所述签名信息;

[0180] 发送模块1204,用于将所述业务数据记录请求发送至所述数据共享系统中的至少一个节点。

[0181] 在一种可能实现方式中,该提取模块1202用于识别生成所述业务处理请求的数据类型;根据所述数据库类型,从数据库类型与表结构的对应关系中,确定生成所述业务处理请求所采用的表结构;基于生成所述业务处理请求所采用的表结构,从所述业务处理请求的对应字段中提取所述用户的业务数据和所述签名信息。

[0182] 在一种可能实现方式中,用户客户端获取所述用户基于所述表结构所输入的业务数据;

[0183] 所述用户客户端从该用户客户端中获取所述用户的私钥,并采用所述私钥对所述业务数据进行签名,得到所述用户的签名信息;将所述业务数据和所述用户的签名信息封装为所述业务处理请求。

[0184] 在一种可能实现方式中,该数据共享系统的节点包括:

[0185] 特征值生成模块,用于接收到所述业务数据记录请求时,根据所述用户的业务数据、所述签名信息生成当前区块的特征值;

[0186] 区块生成模块,用于基于所述用户的业务数据、所述签名信息、区块链中前一区块的特征值以及当前区块的特征值,生成所述当前区块。

[0187] 在一种可能实现方式中,该区块生成模块包括:

[0188] 拆分子模块,用于将所述用户的业务数据、所述签名信息分为至少两部分数据;

[0189] 计算子模块,用于对所述至少两部分数据分别采用不同的哈希算法进行计算,得到所述至少两部分数据的哈希值;

[0190] 拼接子模块,用于将所述至少两部分数据的哈希值拼接,得到所述当前区块的特征值。

[0191] 在一种可能实现方式中,该拆分子模块用于根据所述用户的业务数据、所述签名信息的数据量,确定待分割的份数;将所述用户的业务数据、所述签名信息分为所确定的份数的数据。

[0192] 在一种可能实现方式中,该区块生成模块用于采用节点的私钥对所述用户的业务数据、所述签名信息、所述区块链中前一区块的特征值以及当前区块的特征值进行签名,得到所述当前区块的签名信息;将所述用户的业务数据、所述签名信息、所述区块链中前一区块的特征值、当前区块的特征值以及所述当前区块的签名信息对应存储,生成所述当前区块。

[0193] 在一种可能实现方式中,所述业务数据包括合约数据,所述合约数据包括合约的执行条件参数以及执行参数。

[0194] 在一种可能实现方式中,所述合约数据为包括函数名和参数的二进制代码;或,所述合约数据为脚本代码。

[0195] 在一种可能实现方式中,所述节点还包括合约执行模块,用于如果满足所述执行条件参数,基于所述执行参数执行所述合约数据所指示的业务处理。

[0196] 图13是本发明实施例提供的一种业务处理装置的结构示意图。参见图13,所述装置包括:

[0197] 接收模块1301,用于接收用户客户端的业务处理请求,所述业务处理请求携带业务数据以及所述用户客户端的公钥,所述业务数据包括所述用户客户端的地址信息;

[0198] 生成模块1302,用于根据所述用户客户端的公钥,生成所述用户客户端的校验地址信息;

[0199] 业务请求处理模块1303,用于如果所述用户客户端的校验地址信息和所述业务数据所包括的地址信息一致,则响应所述业务处理请求,如果不一致,则拦截所述业务处理请求。

[0200] 在一种可能实现方式中,该生成模块1302包括:

[0201] 公钥哈希值获取子模块,用于获取所述用户客户端的公钥哈希值;

[0202] 哈希值获取子模块,用于对所述公钥哈希值进行至少两次哈希运算,得到所述公钥哈希值的哈希值;

[0203] 校验码获取子模块,用于从所述公钥哈希值的哈希值中提取前预设位数的字节作为校验码;

[0204] 地址信息获取子模块,用于将所述公钥哈希值和所述校验码进行拼接,并对拼接得到的字符串进行符合所述数据共享系统所支持的数据格式的编码处理,得到所述用户客户端的地址信息。

[0205] 在一种可能实现方式中,该地址信息获取子模块用于将所述数据共享系统的版本信息、所述公钥哈希值和所述校验码进行拼接。

[0206] 在一种可能实现方式中,所述业务处理请求还包括签名信息,所述签名信息由所述用户客户端采用所述用户客户端的私钥对所述业务数据进行签名得到。

[0207] 图14是本发明实施例提供的一种业务处理装置的结构示意图。参见图14,所述装置包括:

[0208] 业务数据获取模块1401,用于获取业务数据;

[0209] 私钥获取模块1402,用于获取用户客户端的私钥;

[0210] 签名模块1403,用于采用所述用户客户端的私钥对所述业务数据进行签名,得到所述用户客户端的签名信息;

[0211] 公钥生成模块1404,用于根据所述用户客户端的私钥生成所述用户客户端的公钥;

[0212] 请求发送模块1405,用于将所述业务数据、所述用户客户端的签名信息和所述用户客户端的公钥封装为业务处理请求,并向数据共享系统发送所述业务处理请求。

[0213] 在一种可能实现方式中,所述私钥获取模块包括:

[0214] 随机数生成子模块,用于采用非对称加密算法,生成第一指定位数的随机数;

[0215] 扩展子模块,用于将该第一指定位数的随机数进行位数扩展,得到第二指定位数的随机数。

[0216] 在一种可能实现方式中,该扩展子模块用于将两个该第一指定位数的随机数进行拼接,得到第二指定位数的随机数。

[0217] 在一种可能实现方式中,该扩展子模块用于将一个所述第一指定位数的随机数的尾部和另一个所述第一指定位数的随机数的头部相连,得到所述第二指定位数的随机数;或,

[0218] 将一个所述第一指定位数的随机数中预设位数的字符与另一个所述第一指定位数的随机数中所述预设位数的字符插空混合,得到所述第二指定位数的随机数;或,

[0219] 将一个所述第一指定位数的随机数和另一个所述第一指定位数的随机数的字符打乱,得到所述第二指定位数的随机数。

[0220] 需要说明的是:上述实施例提供的业务处理装置在业务处理时,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,即将设备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。另外,上述实施例提供的业务处理装置与业务处理方法实施例属于同一构思,其具体实现过程详见方法实施例,这里不再赘述。

[0221] 本实施例提供了一种终端,该终端运行有上述方法中的用户客户端,并用于执行上述各个实施例中提供的业务处理方法。参见图15,该终端1500包括:

[0222] 终端1500可以包括RF (Radio Frequency,射频) 电路110、包括有一个或一个以上计算机可读存储介质的存储器120、输入单元130、显示单元140、传感器150、音频电路160、

WiFi (Wireless Fidelity, 无线保真) 模块170、包括有一个或者一个以上处理核心的处理器180、以及电源190等部件。本领域技术人员可以理解,图15中示出的终端结构并不构成对终端的限定,可以包括比图示更多或更少的部件,或者组合某些部件,或者不同的部件布置。其中:

[0223] RF电路110可用于收发信息或通话过程中,信号的接收和发送,特别地,将基站的下行信息接收后,交由一个或者一个以上处理器180处理;另外,将涉及上行的数据发送给基站。通常,RF电路110包括但不限于天线、至少一个放大器、调谐器、一个或多个振荡器、用户身份模块(SIM)卡、收发信机、耦合器、LNA(Low Noise Amplifier,低噪声放大器)、双工器等。此外,RF电路110还可以通过无线通信与网络和其他设备通信。所述无线通信可以使用任一通信标准或协议,包括但不限于GSM(Global System of Mobile communication,全球移动通讯系统)、GPRS(General Packet Radio Service,通用分组无线服务)、CDMA(Code Division Multiple Access,码分多址)、WCDMA(Wideband Code Division Multiple Access,宽带码分多址)、LTE(Long Term Evolution,长期演进)、电子邮件、SMS(Short Messaging Service,短消息服务)等。

[0224] 存储器120可用于存储软件程序以及模块,处理器180通过运行存储在存储器120的软件程序以及模块,从而执行各种功能应用以及数据处理。存储器120可主要包括存储程序区和存储数据区,其中,存储程序区可存储操作系统、至少一个功能所需的应用程序(比如声音播放功能、图像播放功能等)等;存储数据区可存储根据终端1500的使用所创建的数据(比如音频数据、电话本等)等。此外,存储器120可以包括高速随机存取存储器,还可以包括非易失性存储器,例如至少一个磁盘存储器件、闪存器件、或其他易失性固态存储器件。相应地,存储器120还可以包括存储器控制器,以提供处理器180和输入单元130对存储器120的访问。

[0225] 输入单元130可用于接收输入的数字或字符信息,以及产生与用户设置以及功能控制有关的键盘、鼠标、操作杆、光学或者轨迹球信号输入。具体地,输入单元130可包括触敏表面131以及其他输入设备132。触敏表面131,也称为触摸显示屏或者触控板,可收集用户在其上或附近的触摸操作(比如用户使用手指、触笔等任何适合的物体或附件在触敏表面131上或在触敏表面131附近的操作),并根据预先设定的程式驱动相应的连接装置。可选的,触敏表面131可包括触摸检测装置和触摸控制器两个部分。其中,触摸检测装置检测用户的触摸方位,并检测触摸操作带来的信号,将信号传送给触摸控制器;触摸控制器从触摸检测装置上接收触摸信息,并将它转换成触点坐标,再送给处理器180,并能接收处理器180发来的命令并加以执行。此外,可以采用电阻式、电容式、红外线以及表面声波等多种类型实现触敏表面131。除了触敏表面131,输入单元130还可以包括其他输入设备132。具体地,其他输入设备132可以包括但不限于物理键盘、功能键(比如音量控制按键、开关按键等)、轨迹球、鼠标、操作杆等中的一种或多种。

[0226] 显示单元140可用于显示由用户输入的信息或提供给用户的信息以及终端1500的各种图形用户接口,这些图形用户接口可以由图形、文本、图标、视频和其任意组合来构成。显示单元140可包括显示面板141,可选的,可以采用LCD(Liquid Crystal Display,液晶显示器)、OLED(Organic Light-Emitting Diode,有机发光二极管)等形式来配置显示面板141。进一步的,触敏表面131可覆盖显示面板141,当触敏表面131检测到在其上或附近的触

摸操作后,传送给处理器180以确定触摸事件的类型,随后处理器180根据触摸事件的类型在显示面板141上提供相应的视觉输出。虽然在图15中,触敏表面131与显示面板141是作为两个独立的部件来实现输入和输出功能,但是在某些实施例中,可以将触敏表面131与显示面板141集成而实现输入和输出功能。

[0227] 终端1500还可包括至少一种传感器150,比如光传感器、运动传感器以及其他传感器。具体地,光传感器可包括环境光传感器及接近传感器,其中,环境光传感器可根据环境光线的明暗来调节显示面板141的亮度,接近传感器可在终端1500移动到耳边时,关闭显示面板141和/或背光。作为运动传感器的一种,重力加速度传感器可检测各个方向上(一般为三轴)加速度的大小,静止时可检测出重力的大小及方向,可用于识别手机姿态的应用(比如横竖屏切换、相关游戏、磁力计姿态校准)、振动识别相关功能(比如计步器、敲击)等;至于终端1500还可配置的陀螺仪、气压计、湿度计、温度计、红外线传感器等其他传感器,在此不再赘述。

[0228] 音频电路160、扬声器161,传声器162可提供用户与终端1500之间的音频接口。音频电路160可将接收到的音频数据转换后的电信号,传输到扬声器161,由扬声器161转换为声音信号输出;另一方面,传声器162将收集的声音信号转换为电信号,由音频电路160接收后转换为音频数据,再将音频数据输出处理器180处理后,经RF电路110以发送给比如另一终端,或者将音频数据输出至存储器120以便进一步处理。音频电路160还可能包括耳塞插孔,以提供外设耳机与终端1500的通信。

[0229] WiFi属于短距离无线传输技术,终端1500通过WiFi模块170可以帮助用户收发电子邮件、浏览网页和访问流式媒体等,它为用户提供了无线的宽带互联网访问。虽然图15示出了WiFi模块170,但是可以理解的是,其并不属于终端1500的必须构成,完全可以根据需要在不改变发明的本质的范围内而省略。

[0230] 处理器180是终端1500的控制中心,利用各种接口和线路连接整个手机的各个部分,通过运行或执行存储在存储器120内的软件程序和/或模块,以及调用存储在存储器120内的数据,执行终端1500的各种功能和处理数据,从而对手机进行整体监控。可选的,处理器180可包括一个或多个处理核心;优选的,处理器180可集成应用处理器和调制解调处理器,其中,应用处理器主要处理操作系统、用户界面和应用程序等,调制解调处理器主要处理无线通信。可以理解的是,上述调制解调处理器也可以不集成到处理器180中。

[0231] 终端1500还包括给各个部件供电的电源190(比如电池),优选的,电源可以通过电源管理系统与处理器180逻辑相连,从而通过电源管理系统实现管理充电、放电、以及功耗管理等功能。电源190还可以包括一个或一个以上的直流或交流电源、再充电系统、电源故障检测电路、电源转换器或者逆变器、电源状态指示器等任意组件。

[0232] 尽管未示出,终端1500还可以包括摄像头、蓝牙模块等,在此不再赘述。具体在本实施例中,终端的显示单元是触摸屏显示器,终端还包括有存储器,以及一个或者一个以上的程序,其中一个或者一个以上程序存储于存储器中,且经配置以由一个或者一个以上处理器执行。所述一个或者一个以上程序包含用于执行该业务处理方法中用户客户端操作的指令。

[0233] 图16是根据一示例性实施例示出的一种业务处理装置1600的框图。例如,装置1600可以被提供为数据共享系统中的数据共享系统网关或节点。参照图16,装置1600包括

处理组件1622，其进一步包括一个或多个处理器，以及由存储器1632所代表的存储器资源，用于存储可由处理部件1622执行的指令，例如应用程序。存储器1632中存储的应用程序可以包括一个或一个以上的每一个对应于一组指令的模块。此外，处理组件1622被配置为执行指令，以执行上述业务处理方法。

[0234] 装置1600还可以包括一个电源组件1626被配置为执行装置1600的电源管理，一个有线或无线网络接口1650被配置为将装置1600连接到网络，和一个输入输出(I/O)接口1658。装置1600可以操作基于存储在存储器1632的操作系统，例如Windows Server<sup>TM</sup>, Mac OS X<sup>TM</sup>, Unix<sup>TM</sup>, Linux<sup>TM</sup>, FreeBSD<sup>TM</sup>或类似。

[0235] 在示例性实施例中，还提供了一种包括指令的非临时性计算机可读存储介质，例如包括指令的存储器，上述指令可由终端中的处理器执行以完成下述实施例中的资源发放方法或资源领取方法。例如，所述非临时性计算机可读存储介质可以是ROM、随机存取存储器(RAM)、CD-ROM、磁带、软盘和光数据存储设备等。

[0236] 本领域普通技术人员可以理解实现上述实施例的全部或部分步骤可以通过硬件来完成，也可以通过程序来指令相关的硬件完成，所述的程序可以存储于一种计算机可读存储介质中，上述提到的存储介质可以是只读存储器，磁盘或光盘等。

[0237] 以上所述仅为本发明的较佳实施例，并不用以限制本发明，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。

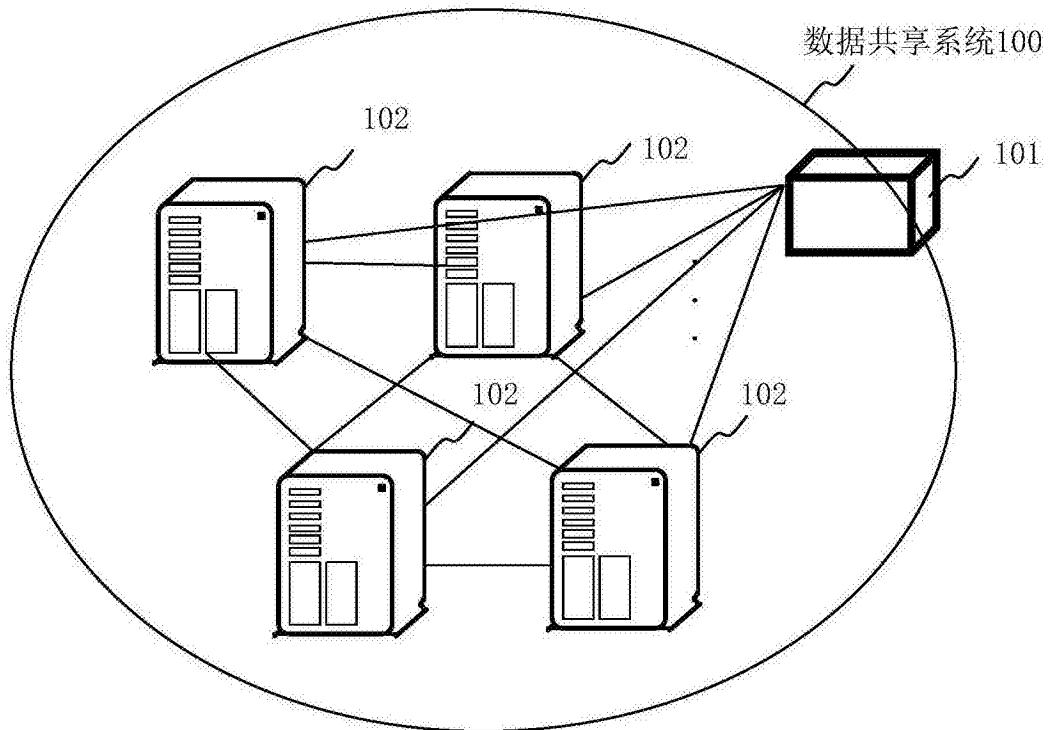


图1

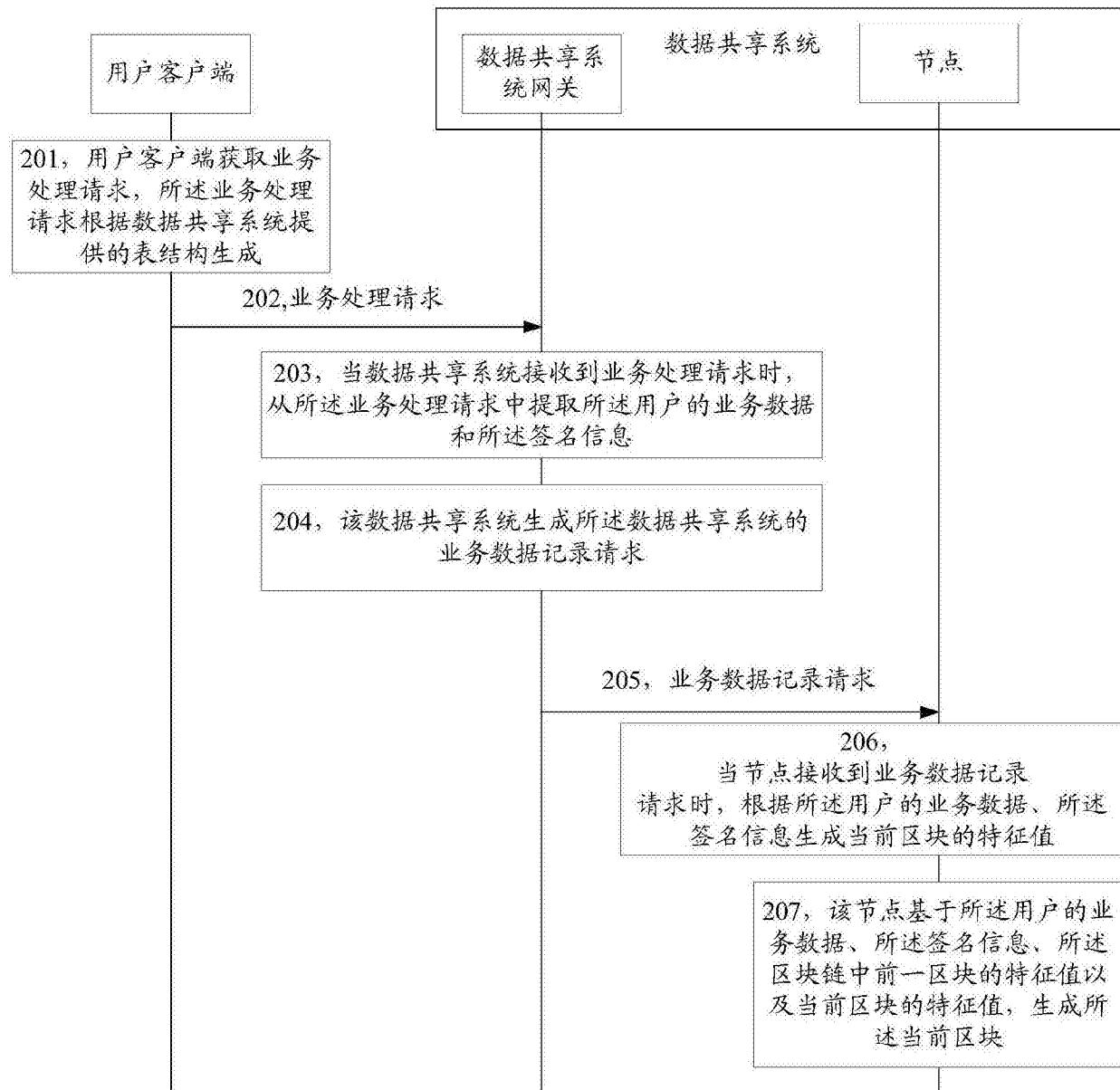


图2

```
[root@CENTOS64 ~]# mysql -uroot -proot
mysql: [warning] Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 3073
Server version: 5.7.18 source distribution

Copyright (c) 2000, 2016, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| bc_cp_db          |
| charmysql          |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
6 rows in set (0.01 sec)
```

```
mysql: [warning] Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 37
Server version: chainsql-0.1-RELEASE chainsql server (ChainSQL)
Copyright (c) 2000, 2016, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;
+-----+
| DATABASE |
+-----+
| chainsql |
+-----+
1 row in set (0.00 sec)
```

图3

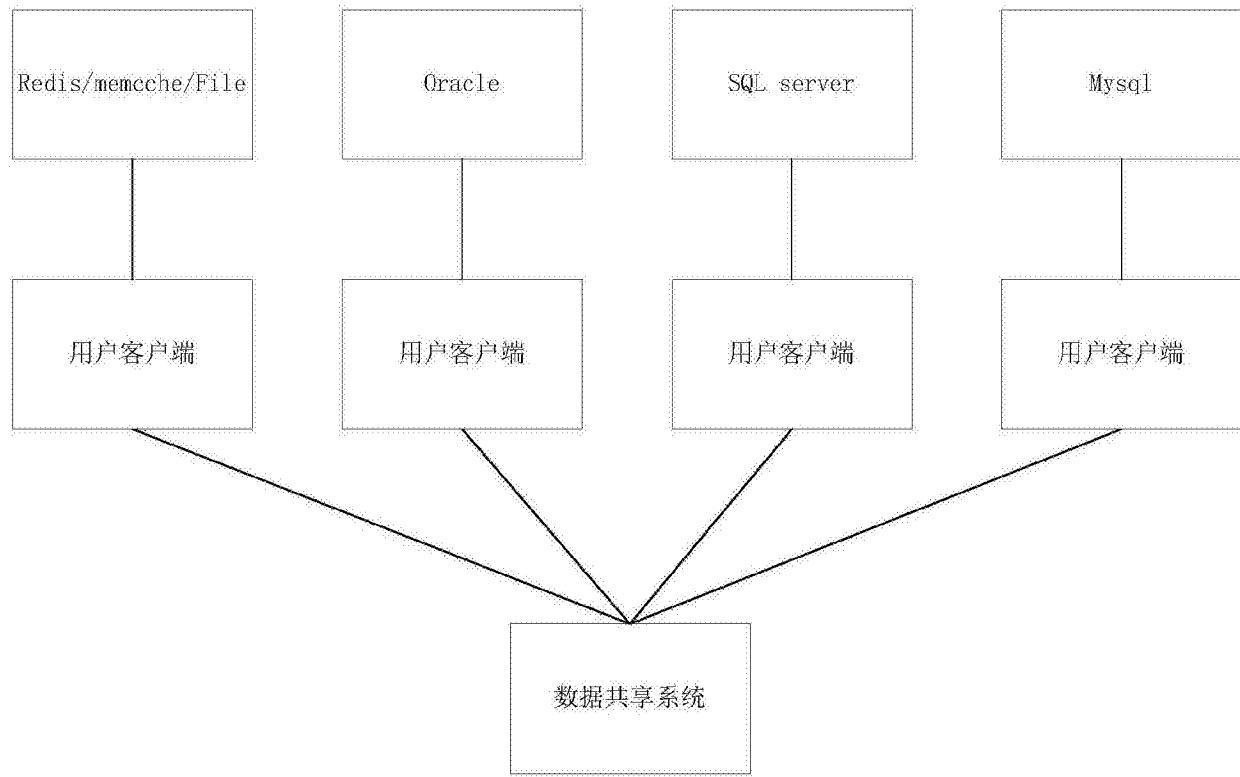


图4

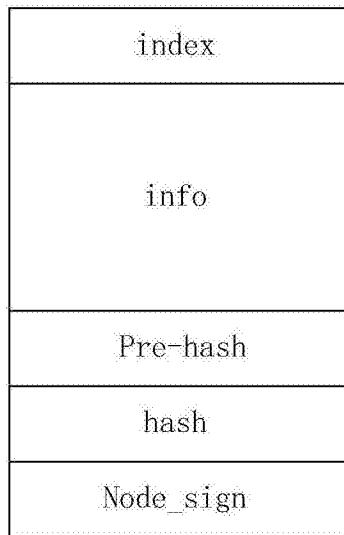


图5

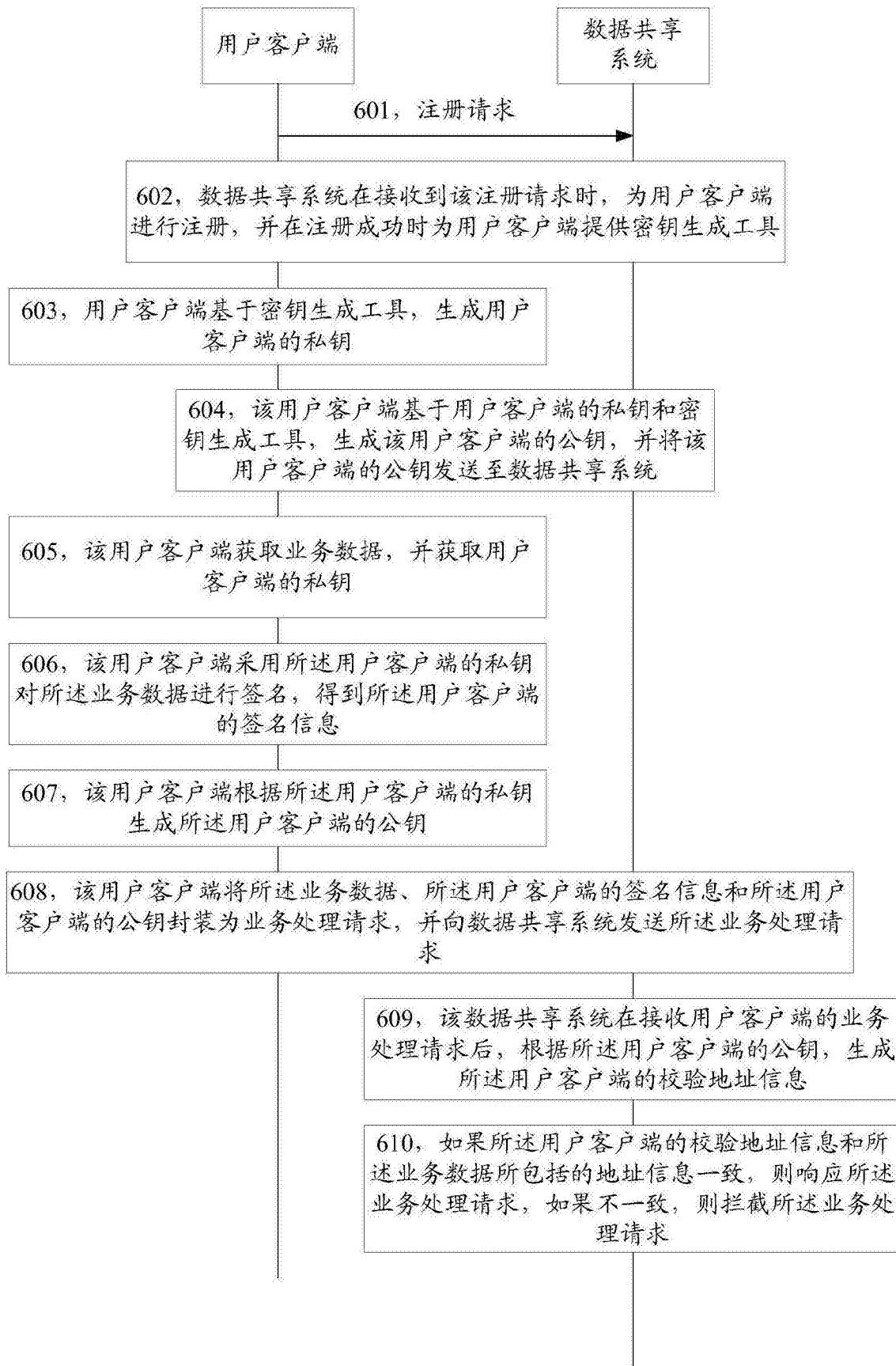


图6

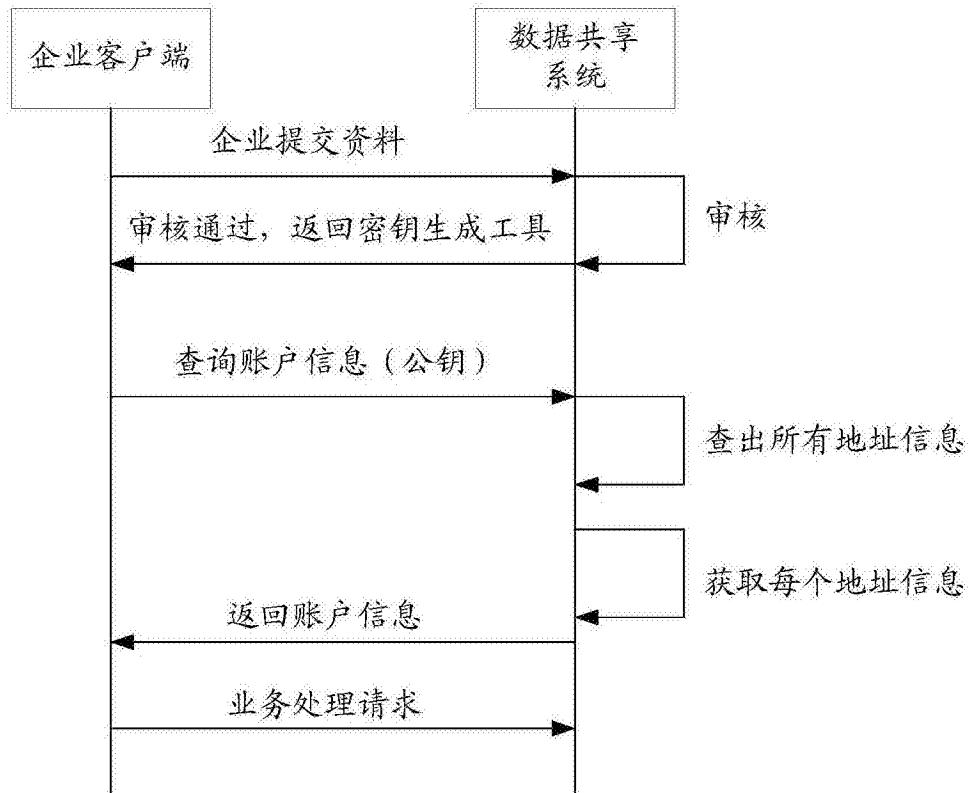


图7

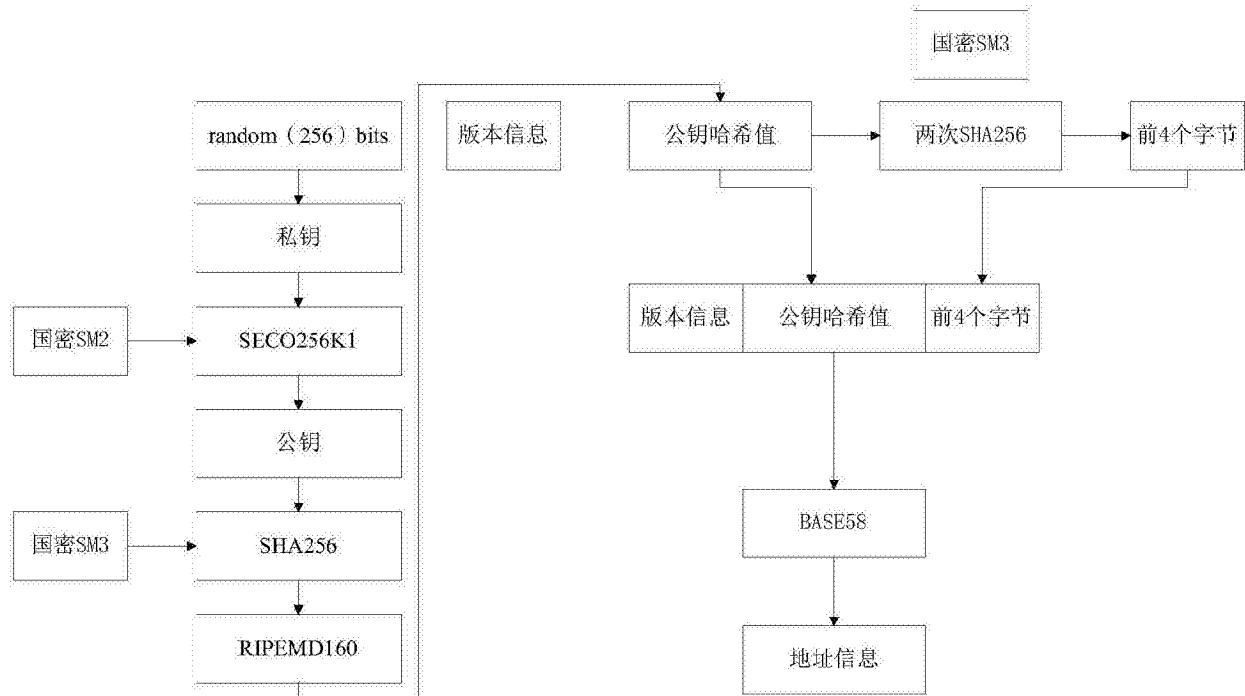


图8

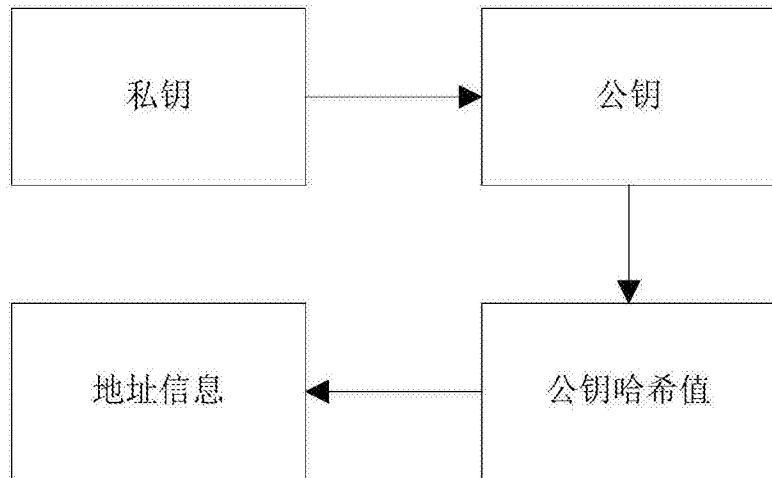


图9

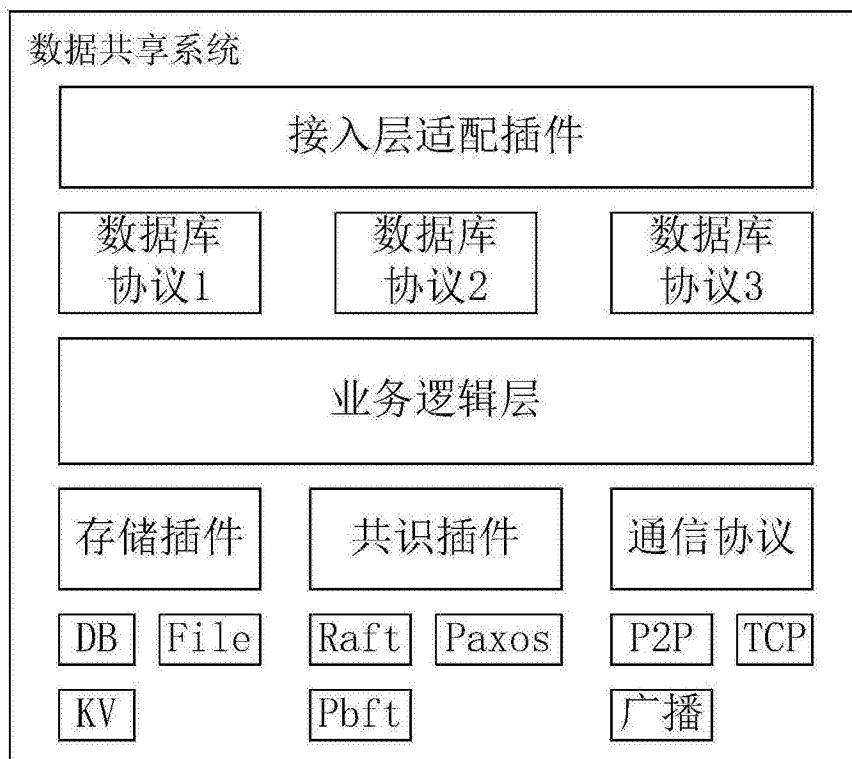


图10

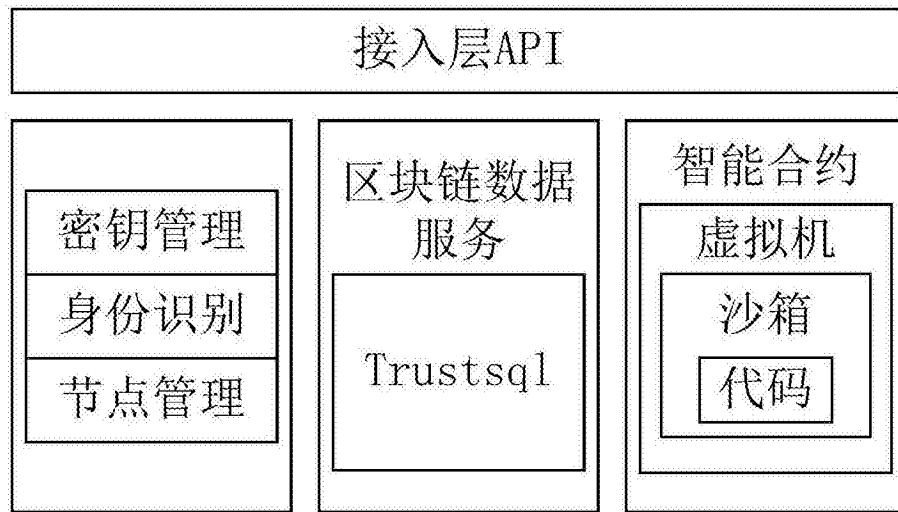


图11

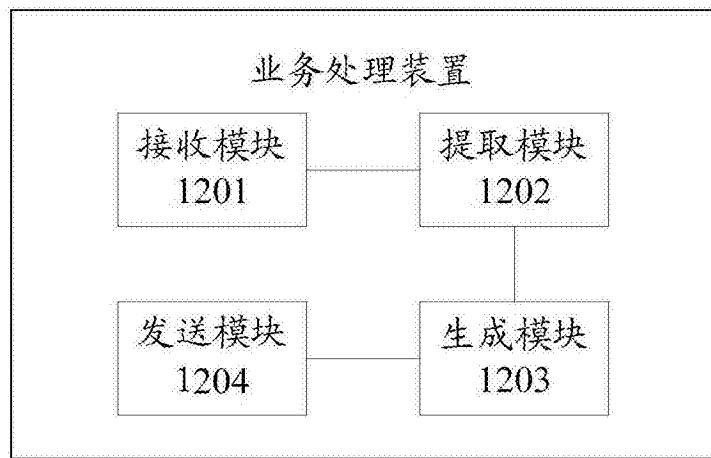


图12

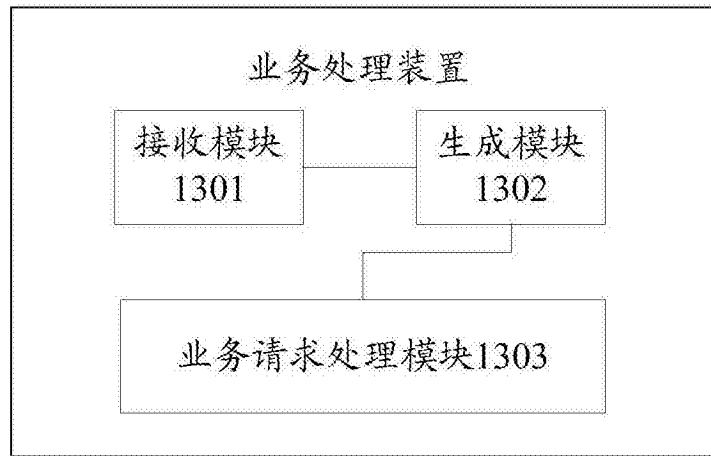


图13

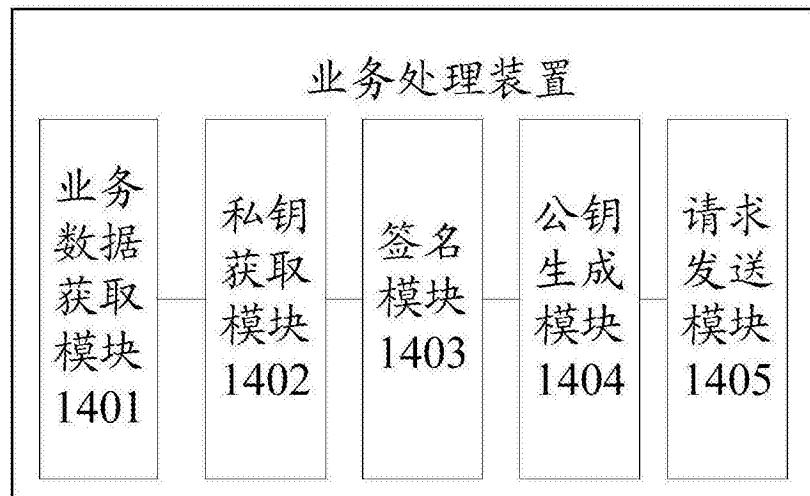


图14

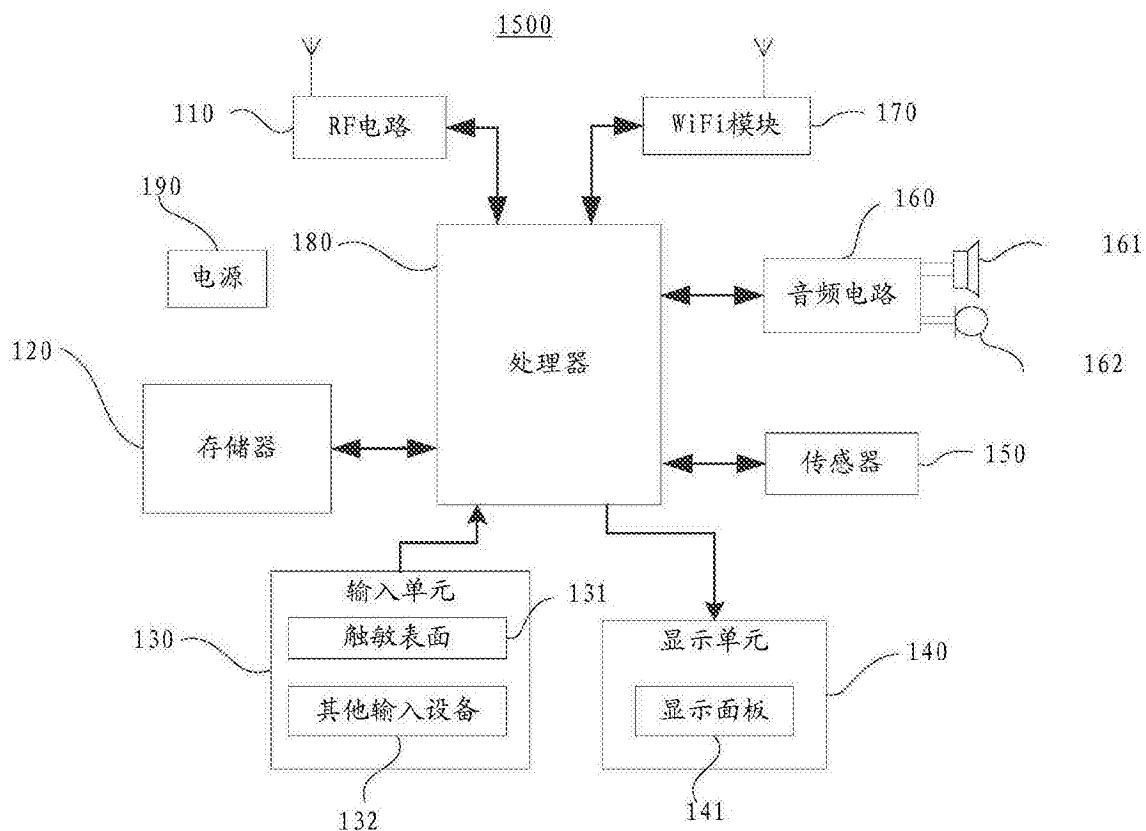


图15

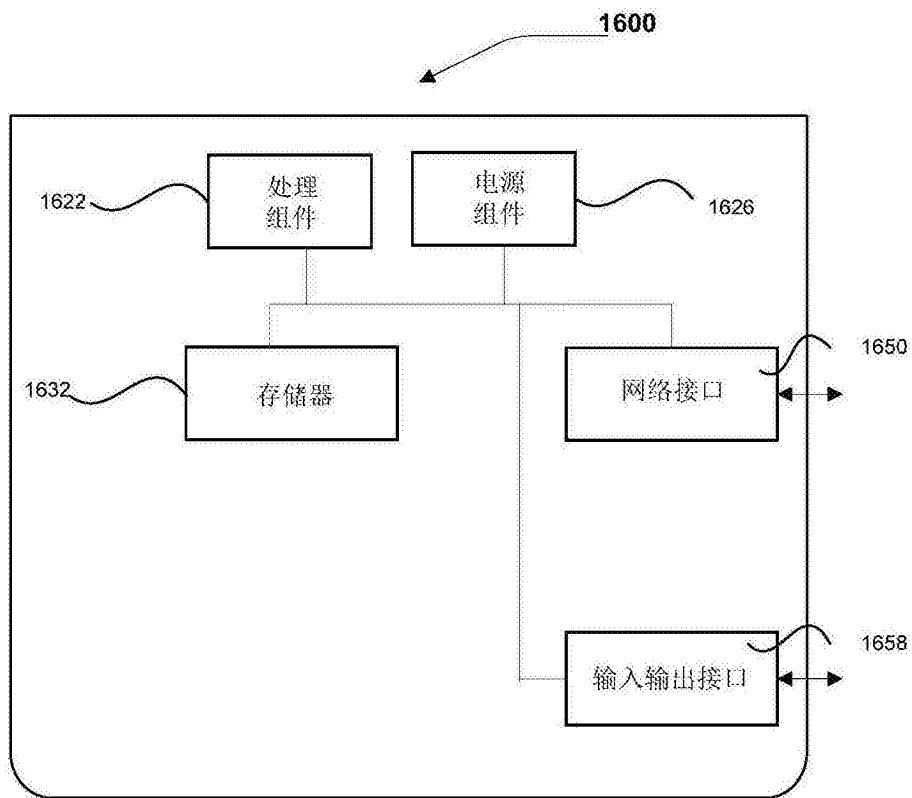


图16