



(12)发明专利申请

(10)申请公布号 CN 108776929 A

(43)申请公布日 2018. 11. 09

(21)申请号 201810285488.5

(22)申请日 2018.04.02

(71)申请人 成都云创智融科技有限公司

地址 610000 四川省成都市高新区中和油  
榨房街65-71号2层202号

(72)发明人 钱路芳

(74)专利代理机构 深圳市世纪恒程知识产权代  
理事务所 44287

代理人 胡海国 晏波

(51) Int. Cl.

G06Q 40/04(2012.01)

G06Q 20/38(2012.01)

G06Q 20/42(2012.01)

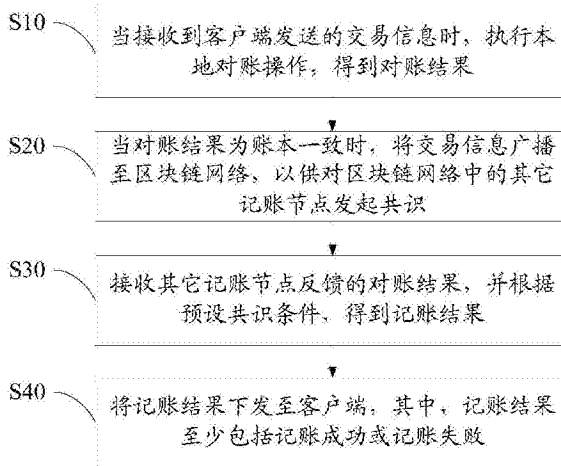
权利要求书2页 说明书10页 附图3页

(54)发明名称

基于区块链数据库的账单处理方法、系统和  
可读存储介质

(57)摘要

本发明公开了一种基于区块链数据库的账  
单处理方法,应用于数据记账系统,所述数据记  
账系统设有多个记账节点,所述方法包括以下步  
骤:当接收到客户端发送的交易信息时,执行本  
地对账操作,得到对账结果;当对账结果为账本  
一致时,将所述交易信息广播至区块链网络,以  
供对区块链网络中的其它记账节点发起共识;接  
收其它记账节点反馈的对账结果,并根据预设共  
识条件,得到记账结果;将所述记账结果下发至  
客户端,其中,所述记账结果至少包括记账成功  
或记账失败。本发明还公开了一种系统和可读存  
储介质。本发明提高了数据处理的效率,进而降  
低资源消耗。



1. 一种基于区块链数据库的账单处理方法,其特征在于,应用于数据记账系统,所述数据记账系统设有多个记账节点,所述基于区块链数据库的账单处理方法包括以下步骤:

当接收到客户端发送的交易信息时,执行本地对账操作,得到对账结果;

当对账结果为账本一致时,将所述交易信息广播至区块链网络,以供对区块链网络中的其它记账节点发起共识;

接收其它记账节点反馈的对账结果,并根据预设共识条件,得到记账结果;

将所述记账结果下发至客户端,其中,所述记账结果至少包括记账成功或记账失败。

2. 如权利要求1所述的基于区块链数据库的账单处理方法,其特征在于,所述当接收到客户端发送的交易信息时,执行本地对账操作,得到对账结果包括:

当接收到客户端发送的交易信息时,确定该客户端为交易发起端并确定交易发起端的交易ID;

在本地区块数据库中,查找与所述交易发起端的交易ID对应的公钥,以供对所述交易信息的私钥进行验证;

当所述公钥与所述私钥一致时,解读所述交易信息的交易内容,得到交易接收端的交易ID和交易金额;

基于所述交易发起端的交易ID和所述交易接收端的交易ID,得到本地区块数据库中记录的账户余额;

基于所述账户余额和所述交易金额,判断交易双方的收支是否相等;

若收支相等,则对账结果为账本一致;

若收支不相等,则对账结果为账本不一致。

3. 如权利要求1所述的基于区块链数据库的账单处理方法,其特征在于,所述接收其它记账节点反馈的对账结果,并根据预设共识条件,得到记账结果包括:

接收其它记账节点反馈的对账结果,并累计计算数量;

获取区块链网络中处于在线的记账节点的总数以及当前调剂值,用以计算接收节点数;

监测在预设时间内累计计算的数量是否大于或等于所述接收节点数;

若在预设时间内累计计算的数量大于或等于所述接收节点数,则基于接收的其它各记账节点的参与度,计算共识值;

判断所述共识值是否大于或等于所述接收节点数;

若所述共识值大于或等于所述接收节点数,则确定共识达成一致,并确定记账结果为记账成功;

若所述共识值小于所述接收节点数,则确定共识不一致,并确定记账结果为记账失败;

若在预设时间内累计计算的数量小于所述接收节点数,则确定网络等待超时,并确定记账结果为记账失败。

4. 如权利要求3所述的基于区块链数据库的账单处理方法,其特征在于,所述基于区块链数据库的账单处理方法还包括:

当共识达成一致时,基于所述交易信息、以及参与本次共识的记账节点,更新本地区块数据库中的交易数据。

5. 如权利要求3所述的基于区块链数据库的账单处理方法,其特征在于,所述基于区块

链数据库的账单处理方法还包括：

当记账结果为记账失败时，向客户端发送失败原因的提示信息，以供用户进行查看。

6. 如权利要求1至5中任一项所述的基于区块链数据库的账单处理方法，其特征在于，所述基于区块链数据库的账单处理方法还包括：

当接收到客户端发送的查询请求时，执行本地区块数据的查询操作，并将所述查询请求广播至区块链网络进行共识，以供确定查询结果，其中，所述查询结果至少包括交易明细；

当共识完成且达成一致时，向客户端返回查询结果；

当共识完成且不一致时，向客户端下发查询失败以及共识失败的提示信息；

当等待共识完成的时长超过预设时长时，向客户端下发查询失败以及网络等待超时的提示信息。

7. 一种数据记账系统，其特征在于，所述数据记账系统包括多个记账节点，以及与所述记账节点建立通信连接的客户端，所述记账节点包括处理器、存储器及存储在所述存储器上并可在所述处理器上运行的账单处理程序，所述账单处理程序被所述处理器执行时实现如权利要求1至6中任一项所述的基于区块链数据库的账单处理方法的步骤。

8. 如权利要求7所述的数据记账系统，其特征在于，所述客户端用于：

基于预置功能选项，编辑交易内容，并采用预存的私钥对所述交易内容进行加密和签名，得到交易信息；

基于所述交易信息，向区块链网络发起交易记账，以供区块链网络中的任一记账节点接收并进行处理。

9. 如权利要求7或8所述的数据记账系统，其特征在于，所述客户端还用于：

基于预置功能选项，编辑查询指令，其中，所述查询指令至少包括交易ID、交易明细的关键字段；

基于所述查询指令，向区块链网络发起查询请求，以供区块链网络中的任一记账节点接收并进行处理。

10. 一种计算机可读存储介质，其特征在于，所述计算机可读存储介质上存储有账单处理程序，所述账单处理程序被处理器执行时实现如权利要求1至6中任一项所述的基于区块链数据库的账单处理方法的步骤。

## 基于区块链数据库的账单处理方法、系统和可读存储介质

### 技术领域

[0001] 本发明涉及区块链技术领域,尤其涉及一种基于区块链数据库的账单处理方法、系统和可读存储介质。

### 背景技术

[0002] 传统交易系统在处理交易账单时,是通过异步通讯方式将网络中多个主机组成网络集群进行协作,而这种异步网络容易被篡改,使得交易数据不可靠。随着区块链技术的兴起与发展,其应用数量和场景急剧增加。区块链是一种由多方共同维护,以块链结构存储数据,并使用密码学保证交易数据传输和访问的安全性,但采用区块链技术,还需要采取一种机制,以保证网络中各主机的状态最终达成相同一致性,即取得共识,从而实现区块数据同步。而随着交易吞吐量的日益增加,导致资源消耗大、数据处理的效率降低,进而使区块数据同步难并延长交易确认时间。

### 发明内容

[0003] 本发明的主要目的在于提供一种基于区块链数据库的账单处理方法、系统和可读存储介质,旨在现有的区块数据处理方式效率低,资源消耗大的技术问题。

[0004] 为实现上述目的,本发明提供了一种基于区块链数据库的账单处理方法,应用于数据记账系统,所述数据记账系统设有多个记账节点,所述基于区块链数据库的账单处理方法包括以下步骤:

[0005] 当接收到客户端发送的交易信息时,执行本地对账操作,得到对账结果;

[0006] 当对账结果为账本一致时,将所述交易信息广播至区块链网络,以供对区块链网络中的其它记账节点发起共识;

[0007] 接收其它记账节点反馈的对账结果,并根据预设共识条件,得到记账结果;

[0008] 将所述记账结果下发至客户端,其中,所述记账结果至少包括记账成功或记账失败。

[0009] 优选地,所述当接收到客户端发送的交易信息时,执行本地对账操作,得到对账结果包括:

[0010] 当接收到客户端发送的交易信息时,确定该客户端为交易发起端并确定交易发起端的交易ID;

[0011] 在本地区块数据库中,查找与所述交易发起端的交易ID对应的公钥,以供对所述交易信息的私钥进行验证;

[0012] 当所述公钥与所述私钥一致时,解读所述交易信息的交易内容,得到交易接收端的交易ID和交易金额;

[0013] 基于所述交易发起端的交易ID和所述交易接收端的交易ID,得到本地区块数据库中记录的账户余额;

[0014] 基于所述账户余额和所述交易金额,判断交易双方的收支是否相等;

- [0015] 若收支相等,则对账结果为账本一致;
- [0016] 若收支不相等,则对账结果为账本不一致。
- [0017] 优选地,所述接收其它记账节点反馈的对账结果,并根据预设共识条件,得到记账结果包括:
- [0018] 接收其它记账节点反馈的对账结果,并累计计算数量;
- [0019] 获取区块链网络中处于在线的记账节点的总数以及当前调剂值,用以计算接收节点数;
- [0020] 监测在预设时间内累计计算的数量是否大于或等于所述接收节点数;
- [0021] 若在预设时间内累计计算的数量大于或等于所述接收节点数,则基于接收的其它各记账节点的参与度,计算共识值;
- [0022] 判断所述共识值是否大于或等于所述接收节点数;
- [0023] 若所述共识值大于或等于所述接收节点数,则确定共识达成一致,并确定记账结果为记账成功;
- [0024] 若所述共识值小于所述接收节点数,则确定共识不一致,并确定记账结果为记账失败;
- [0025] 若在预设时间内累计计算的数量小于所述接收节点数,则确定网络等待超时,并确定记账结果为记账失败。
- [0026] 优选地,所述基于区块链数据库的账单处理方法还包括:
- [0027] 当共识达成一致时,基于所述交易信息、以及参与本次共识的记账节点,更新本地区块数据库中的交易数据。
- [0028] 优选地,所述基于区块链数据库的账单处理方法还包括:
- [0029] 当记账结果为记账失败时,向客户端发送失败原因的提示信息,以供用户进行查看。
- [0030] 优选地,所述基于区块链数据库的账单处理方法还包括:
- [0031] 当接收到客户端发送的查询请求时,执行本地区块数据的查询操作,并将所述查询请求广播至区块链网络进行共识,以供确定查询结果,其中,所述查询结果至少包括交易明细;
- [0032] 当共识完成且达成一致时,向客户端返回查询结果;
- [0033] 当共识完成且不一致时,向客户端下发查询失败以及共识失败的提示信息;
- [0034] 当等待共识完成的时长超过预设时长时,向客户端下发查询失败以及网络等待超时的提示信息。
- [0035] 此外,为实现上述目的,本发明还提供一种数据记账系统,所述数据记账系统包括多个记账节点,以及与所述记账节点建立通信连接的客户端,所述记账节点包括处理器、存储器及存储在所述存储器上并可在所述处理器上运行的账单处理程序,所述账单处理程序被所述处理器执行时实现如上述中任一项所述的基于区块链数据库的账单处理方法的步骤。
- [0036] 优选地,所述客户端用于:
- [0037] 基于预置功能选项,编辑交易内容,并采用预存的私钥对所述交易内容进行加密和签名,得到交易信息;

[0038] 基于所述交易信息,向区块链网络发起交易记账,以供区块链网络中的任一记账节点接收并进行处理。

[0039] 优选地,所述客户端还用于:

[0040] 基于预置功能选项,编辑查询指令,其中,所述查询指令至少包括交易ID、交易明细的关键字段;

[0041] 基于所述查询指令,向区块链网络发起查询请求,以供区块链网络中的任一记账节点接收并进行处理。

[0042] 此外,为实现上述目的,本发明还提供一种计算机可读存储介质,所述计算机可读存储介质上存储有账单处理程序,所述账单处理程序被处理器执行时实现如上述中任一项所述的基于区块链数据库的账单处理方法的步骤。

[0043] 本发明提出的基于区块链数据库的账单处理方法,应用于设有多个记账节点的数据记账系统,当其中一个记账节点接收到客户端发送的交易信息时,先执行本地对账操作,得到对账结果,并当对账结果为账本一致时,将交易信息广播至区块链网络,以供对区块链网络中的其它记账节点发起共识,然后接收其它记账节点反馈的对账结果,并根据预设共识条件,得到记账结果,从而将记账成功或失败的结果下发至客户端。本发明通过区块链技术实现账单处理更加安全可靠的有益效果,同时降低资源消耗,提高处理效率,并缩小用户等待交易确认的时间。

## 附图说明

[0044] 图1为本发明实施例方案涉及的记账节点运行环境的结构示意图;

[0045] 图2为本发明数据记账系统一实施例的功能模块示意图;

[0046] 图3为本发明基于区块链数据库的账单处理方法一实施例的流程示意图;

[0047] 图4为本发明基于区块链数据库的账单处理方法另一实施例的流程示意图。

[0048] 本发明目的的实现、功能特点及优点将结合实施例,参照附图做进一步说明。

## 具体实施方式

[0049] 应当理解,此处所描述的具体实施例仅用以解释本发明,并不用于限定本发明。

[0050] 参照图1,图1为本发明实施例方案涉及的记账节点运行环境的结构示意图。

[0051] 本发明实施例记账节点可以是便携计算机,也可以是服务器、虚拟机设备等具有接收数据、访问网络、发起共识等功能的设备。

[0052] 如图1所示,该记账节点可以包括:处理器1001,例如CPU,通信总线1002、用户接口1003,网络接口1004,存储器1005。其中,通信总线1002用于实现这些组件之间的连接通信。用户接口1003可以包括显示屏(Display)、输入单元比如键盘(Keyboard),网络接口1004可选的可以包括标准的有线接口、无线接口(如WI-FI接口)。存储器1005可以是高速RAM存储器,也可以是稳定的存储器(non-volatile memory),例如磁盘存储器。存储器1005可选的还可以是独立于前述处理器1001的存储装置。

[0053] 本领域技术人员可以理解,图1中示出的记账节点的硬件结构并不构成对记账节点的限定,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。

[0054] 如图1所示,作为一种计算机可读存储介质的存储器1005中可以包括操作系统、网

络通信模块、用户接口模块以及计算机程序。其中,操作系统是管理和控制记账节点和软件资源的程序,支持账单处理程序以及其它软件和/或程序的运行。

[0055] 在图1所示的记账节点的硬件结构中,网络接口1004主要用于接入网络;用户接口1003主要用于侦测确认指令和编辑指令等。而处理器1001可以用于调用存储器1005中存储的账单处理程序,并执行以下操作:

[0056] 当接收到客户端发送的交易信息时,执行本地对账操作,得到对账结果;

[0057] 当对账结果为账本一致时,将所述交易信息广播至区块链网络,以供对区块链网络中的其它记账节点发起共识;

[0058] 接收其它记账节点反馈的对账结果,并根据预设共识条件,得到记账结果;

[0059] 将所述记账结果下发至客户端,其中,所述记账结果至少包括记账成功或记账失败。

[0060] 进一步地,所述记账节点通过处理器1001调用存储器1005中存储的账单处理程序,以执行下述操作:

[0061] 当接收到客户端发送的交易信息时,确定该客户端为交易发起端并确定交易发起端的交易ID;

[0062] 在本地区块数据库中,查找与所述交易发起端的交易ID对应的公钥,以供对所述交易信息的私钥进行验证;

[0063] 当所述公钥与所述私钥一致时,解读所述交易信息的交易内容,得到交易接收端的交易ID和交易金额;

[0064] 基于所述交易发起端的交易ID和所述交易接收端的交易ID,得到本地区块数据库中记录的账户余额;

[0065] 基于所述账户余额和所述交易金额,判断交易双方的收支是否相等;

[0066] 若收支相等,则对账结果为账本一致;

[0067] 若收支不相等,则对账结果为账本不一致。

[0068] 进一步地,所述记账节点通过处理器1001调用存储器1005中存储的账单处理程序,以执行下述操作:

[0069] 接收其它记账节点反馈的对账结果,并累计计算数量;

[0070] 获取区块链网络中处于在线的记账节点的总数以及当前调剂值,用以计算接收节点数;

[0071] 监测在预设时间内累计计算的数量是否大于或等于所述接收节点数;

[0072] 若在预设时间内累计计算的数量大于或等于所述接收节点数,则基于接收的其它各记账节点的参与度,计算共识值;

[0073] 判断所述共识值是否大于或等于所述接收节点数;

[0074] 若所述共识值大于或等于所述接收节点数,则确定共识达成一致,并确定记账结果为记账成功;

[0075] 若所述共识值小于所述接收节点数,则确定共识不一致,并确定记账结果为记账失败;

[0076] 若在预设时间内累计计算的数量小于所述接收节点数,则确定网络等待超时,并确定记账结果为记账失败。

[0077] 进一步地,所述记账节点通过处理器1001调用存储器1005中存储的账单处理程序,以执行下述操作:

[0078] 当共识达成一致时,基于所述交易信息、以及参与本次共识的记账节点,更新本地区块数据库中的交易数据。

[0079] 进一步地,所述记账节点通过处理器1001调用存储器1005中存储的账单处理程序,以执行下述操作:

[0080] 当记账结果为记账失败时,向客户端发送失败原因的提示信息,以供用户进行查看。

[0081] 进一步地,所述记账节点通过处理器1001调用存储器1005中存储的账单处理程序,以执行下述操作:

[0082] 当接收到客户端发送的查询请求时,执行本地区块数据的查询操作,并将所述查询请求广播至区块链网络进行共识,以供确定查询结果,其中,所述查询结果至少包括交易明细;

[0083] 当共识完成且达成一致时,向客户端返回查询结果;

[0084] 当共识完成且不一致时,向客户端下发查询失败以及共识失败的提示信息;

[0085] 当等待共识完成的时长超过预设时长时,向客户端下发查询失败以及网络等待超时的提示信息。

[0086] 本发明还提供一种数据记账系统。

[0087] 参照图2,图2为本发明数据记账系统一实施例的功能模块示意图。

[0088] 本实施例中,数据记账系统包括多个记账节点10以及还包括与记账节点10建立通信连接的客户端20。数据记账系统优选采用分布式部署架构并部署成多个独立的各记账节点10,每个记账节点10可分别与客户端20建立独立的通信连接,用以实现客户端20迅速访问网络并传输数据,如发起交易记账或交易查询等,实现信息交互。

[0089] 进一步地,客户端20用于执行以下操作:

[0090] 步骤A1,基于预置功能选项,编辑交易内容,并采用预存的私钥对交易内容进行加密和签名,得到交易信息;

[0091] 步骤A2,基于交易信息,向区块链网络发起交易记账,以供区块链网络中的任一记账节点接收并进行处理;或

[0092] 步骤B1,基于预置功能选项,编辑查询指令,其中,查询指令至少包括交易ID、交易明细的关键字段;

[0093] 步骤B2,基于查询指令,向区块链网络发起查询请求,以供区块链网络中的任一记账节点接收并进行处理。

[0094] 本实施例中,客户端安装有相应的软件,该软件设置有功能选项,而功能选项为实现应用功能的入口,一般为程序员预先设置好的。每个功能选项对应操作指令,可以是单个也可以是多个组合,从而编辑得到用户选择需要操作的操作指令。需要说明的是,用户在线上资金交易时,首先需要开设一个用户账号,也就是交易ID或账户地址,并在此基础上实现资金交易。比如张三向李四发起一笔交易,交易内容为张三向李四转账100,张三为支出方,李四为接收方(接收方可以多个),张三用自己的私钥加密本次交易的交易金额100得到一串加密字符,然后再用私钥签名本次交易的内容,即得到交易信息。向区块链网络发起



交易记账,即将交易信息发送至区块链网络中的任一记账节点,接收该交易信息的记账节点即可执行对账等操作。进一步地,加密方法与现有的加密方法一致,优选为哈希算法(hash),包括MD5、SHA2等,使得交易信息不可随意篡改,保障了数据的可靠性和安全性。

[0095] 本实施例中,用户还可实时查询自己的账户,交易明细的关键字段如一段时间内的交易明细、当前余额、历史转出或收入多少等。比如发起对张三账户的查询,具体地,查询指令包括张三的交易ID和查询最新的10个交易。向区块链网络发起查询请求,即将查询指令发送至区块链网络中的任一记账节点,接收该查询指令的记账节点即可执行查询等操作。

[0096] 进一步地,客户端在向区块链网络发起交易记账或查询请求后,还接收记账节点返回的信息,如返回的记账成功信息或查询结果等。

[0097] 基于上述记账节点及数据记账系统的硬件结构,提出本发明基于区块链数据库的账单处理方法的各个实施例。

[0098] 参照图3,图3为本发明基于区块链数据库的账单处理方法一实施例的流程示意图。

[0099] 本实施例中,基于区块链数据库的账单处理方法包括以下步骤:

[0100] 步骤S10,当接收到客户端发送的交易信息时,执行本地对账操作,得到对账结果;

[0101] 本实施例中,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,是一种按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构,并以密码学方式保证的不可篡改和不可伪造的分布式账本。同时共识机制是区块链系统中实现不同节点之间建立信任、获取权益的数学算法。具体地,数据记账系统分布式部署有多个独立的记账节点,每个记账节点均可独立完成本地对账、收发信息等。当系统中任一个记账节点接收到客户端发送的交易信息时,首先执行本地对账操作,也就是根据交易信息中交易双方的余额与对应的收支,在本地进行对账,得到对账结果,如账本一致或不一致。为了进一步方便理解本发明方法,将接收客户端发送的交易信息的记账节点标记为节点a,将其它记账节点标记为节点b、c、d...,依次类推。

[0102] 步骤S20,当对账结果为账本一致时,将交易信息广播至区块链网络,以供对区块链网络中的其它记账节点发起共识;

[0103] 本实施例中,共识机制(NNAC,network notify agree consensus),是通过特殊节点的投票,在很短的时间内完成对交易的验证和确认,即对一笔交易,如果利益不相干的若干个记账节点能够达成共识,就可以认为全网对此也能够达成共识。优选所有记账节点超过50%以上的节点达成一致后,才能完成对交易账目的认可和记账。

[0104] 本实施例中,只有当节点a完成本地对账且对账结果a为账本一致时,将交易信息广播至区块链网络,即使在线的其它记账节点接收到节点a发送的交易信息,然后其它记账节点各自进行本地对账,再将各自对账的结果广播出去,实现共识。简单的说就是,其它节点b、c、d均收到节点a广播的交易信息,节点b本地对账,得到对账结果b,并广播至区块链网络,使得节点a、c、d收到,同样节点c本地对账,得到对账结果c,并广播至区块链网络,使得节点a、b、d收到,依次类推。应当理解的是,实际应用中,参与共识的其它记账节点的数量甚至更多,如1000个等,具体根据实际情况进行调整。

[0105] 步骤S30,接收其它记账节点反馈的对账结果,并根据预设共识条件,得到记账结

果；

[0106] 步骤S40,将记账结果下发至客户端,其中,记账结果至少包括记账成功或记账失败。

[0107] 本实施例中,预设共识条件是预先设置好的一套用以判断共识是否达成一致的规则,是预先设置好的一套用以区分不同记账结果的方式。通过广播交易信息,然后再接收参与共识的其它记账节点反馈的对账结果,并采用预设共识条件,得到记账失败或记账成功的结果。将记账结果下发至客户端,以供用户了解交易进度。

[0108] 本实施例中,提出的基于区块链数据库的账单处理方法,应用于设有多个记账节点的数据记账系统,并通过区块链技术实现账单处理更加安全可靠的有益效果,同时降低资源消耗,提高处理效率,并缩小用户等待交易确认的时间。

[0109] 基于上述实施例,本实施例中,上述步骤S10,当接收到客户端发送的交易信息时,执行本地对账操作,得到对账结果,包括:

[0110] 步骤S11,当接收到客户端发送的交易信息时,确定该客户端为交易发起端并确定交易发起端的交易ID;

[0111] 步骤S12,在本地区块数据库中,查找与交易发起端的交易ID对应的公钥,以供对交易信息的私钥进行验证;

[0112] 步骤S13,当公钥与私钥一致时,解读交易信息的交易内容,得到交易接收端的交易ID和交易金额;

[0113] 步骤S14,基于交易发起端的交易ID和交易接收端的交易ID,得到本地区块数据库中记录的账户余额;

[0114] 步骤S15,基于账户余额和交易金额,判断交易双方的收支是否相等;

[0115] 步骤S16,若收支相等,则对账结果为账本一致;

[0116] 步骤S17,若收支不相等,则对账结果为账本不一致。

[0117] 本实施例中,记账节点a接收到客户端发送的交易信息,即可确定该客户端的用户为交易支出方、交易发起方,因而确定该客户端为交易发起端。应当理解的是,每一笔交易必定存在支出方和收款方(对应交易发起端和交易接收端),双方各自有属于自己的账户地址,即交易ID。记账节点的本地区块数据库中存储有多个账户以及与账户相关的交易记录、公钥等数据。由于交易信息为加密数据,因而根据交易发起端的交易ID,在本地区块数据库中查找到与之对应的公钥,用以解密交易信息。比如收到张三发送的交易信息后,首先用张三的公钥验证交易签名,验证通过,再用公钥从加密字符串中还原得到交易金额100,然后根据交易双方账户上的金额总和,判断收支是否相等,如果收支相等,则证明交易有效,可执行下一步共识操作。比如张三(支出方)账户原来有900,支出100后,目前账户余额为800,李四(收款方)账户原来有500,收入100后,目前账户余额为600,即双方的支出和收入相等,本次交易有效。如果收支不相等,直接向张三返回失败,交易结束。

[0118] 基于上述实施例,本实施例中,上述步骤S30,接收其它记账节点反馈的对账结果,并根据预设共识条件,得到记账结果,包括:

[0119] 步骤S31,接收其它记账节点反馈的对账结果,并累计计算数量;

[0120] 步骤S32,获取区块链网络中处于在线的记账节点的总数以及当前调剂值,用以计算接收节点数;

[0121] 步骤S33,监测在预设时间内累计计算的数量是否大于或等于接收节点数;

[0122] 步骤S34,若在预设时间内累计计算的数量大于或等于接收节点数,则基于接收的其它各记账节点的参与度,计算共识值;

[0123] 步骤S35,判断共识值是否大于或等于接收节点数;

[0124] 步骤S36,若共识值大于或等于接收节点数,则确定共识达成一致,并确定记账结果为记账成功;

[0125] 步骤S37,若共识值小于接收节点数,则确定共识不一致,并确定记账结果为记账失败;

[0126] 步骤S38,若在预设时间内累计计算的数量小于接收节点数,则确定网络等待超时,并确定记账结果为记账失败。

[0127] 本实施例中,由于将交易信息广播至区块链网络,进而对当前网络在线的其它记账节点发起共识,从而其它记账节点在接收到交易信息后各自完成本地对账,并将对账结果广播出去,从而记账节点a能够接收到其它记账节点反馈的对账结果。同时由于全网在线的记账节点的数量以及最终接收到反馈所对应的记账节点的数量是可变的,因而累计计算接收的对账结果的数量,即得到反馈的记账节点的数量。

[0128] 其中,计算接收节点数的公式为 $x = \frac{N_{\text{总}}}{2} \times 1 + T$

[0129]  $N_{\text{总}}$ 为区块链网络中处于在线的记账节点的总数,此处可通过现有的网络心跳机制实时监测所有在线的记账节点,并统计数量;

[0130]  $T$ 为当前调剂值,此处 $T$ 可根据实际业务需要进行设定,且 $1 \leq T \leq \frac{N_{\text{总}}}{2}$ 。

[0131] 计算共识值的公式为 $y = \sum_1^n N_n \times P_n$

[0132]  $P$ 为记账节点参与度: $P = \frac{q}{m}$  ( $m$ 为本记账节点a记录的全网交易次数, $q$ 为本记账节点记录的该记账节点b、c...等曾经参与记账的共识正确次数。 $P$ 初始值为1, $0 < P \leq 1$ )

[0133] 需要说明的是, $\sum_1^n N_n \times P_n = N_1 \times P_1 + N_2 \times P_2 + \dots + N_n \times P_n$

[0134] 假设当前区块链网络中处于在线的记账节点的总数 $N_{\text{总}}$ 为1000,当前调剂值 $T$ 为1,那么接收节点数计算可得501。在预设时间内未接收到501个记账节点反馈的记账结果,则确定网络等待超时,同时确定记账结果为记账失败。若在预设时间内接收到501个记账节点反馈的记账结果时,即可执行共识计算,且计算的共识值大于或等于501,则说明目前所有记账节点超过50%以上的节点达成一致,即能够完成对本次交易账目的认可和记账,此时确定记账结果为记账成功。若计算的共识值小于501则说明共识未达成一致,此时确定记账结果为记账失败。通过共识保证数据的高可靠性,同时运算成本低,可降低资源消耗,提高效率。

[0135] 进一步可选的,在本发明基于区块链数据库的账单处理方法一实施例中,为更新并同步区块数据,本实施例的基于区块链数据库的账单处理方法还包括:

[0136] 当共识达成一致时,基于交易信息、以及参与本次共识的记账节点,更新本地区块数据库中的交易数据。

[0137] 本实施例中,在共识达成一致时,说明本次交易有效,将共识一致的交易信息,如收支明细更新交易双方的个人账本。将参与本次共识的记账节点,如参与的某一记账节点

编号、共识正确/错误次数、参与全网交易次数等更新对应的历史记录。即将共识多数方的记账点的 $q$ 值更新为 $q+1$ ，将自己本地的记账总交易数 $m$ 值更新为 $m+1$ 。应当理解的是，区块链数据保证数据可靠，因而为了使区块数据同步，即各记账节点均根据共识一致的交易信息、参与本次共识的记账节点，更新各自本地的区块数据库数据，从而使整个区块链网络中的任一区块数据库中存储的数据保持一致性。

[0138] 进一步可选的，在本发明基于区块链数据库的账单处理方法一实施例中，为使用户清楚知悉记账失败的原因，进而更好的解决问题，本实施例的基于区块链数据库的账单处理方法还包括：

[0139] 当记账结果为记账失败时，向客户端发送失败原因的提示信息，以供用户进行查看。

[0140] 本实施例中，在将记账结果下发至客户端的同时，若记账结果为记账失败，还将失败原因的提示信息一并下发给客户端。比如因为网络等待超时，而未接收到足够多的对账结果，即将网络等待超时以及记账失败的提示信息下发至客户端。如因为接收到足够多的对账结果，但共识不一致的，将共识不一致以及记账失败的提示信息下发至客户端。用户通过客户端显示提示信息，即可清楚知悉交易进度，并缩短用户等待交易确认的时间，提高了用户的使用体验。

[0141] 参照图4，图4为本发明基于区块链数据库的账单处理方法另一实施例的流程示意图。

[0142] 基于上述实施例，本实施例中，基于区块链数据库的账单处理方法还包括以下步骤：

[0143] 步骤S50，当接收到客户端发送的查询请求时，执行本地区块数据的查询操作，并将查询请求广播至区块链网络进行共识，以供确定查询结果，其中，查询结果至少包括交易明细；

[0144] 步骤S60，当共识完成且达成一致时，向客户端返回查询结果；

[0145] 步骤S70，当共识完成且不一致时，向客户端下发查询失败以及共识失败的提示信息；

[0146] 步骤S80，当等待共识完成的时长超过预设时长时，向客户端下发查询失败以及网络等待超时的提示信息。

[0147] 本实施例中，查询操作与上述实施例中的记账操作步骤一致，不同的是一个是记账，把数据存储在本地区块数据库中，另一个查询是将数据库中的相关数据返回给客户端，以供用户进行查看。具体地，客户端发起对张三的交易ID的查询，用以查询最新的10笔交易明细。当全网中任一个记账节点接收到客户端发送的查询请求时，根据查询请求，查询本地区块数据库中的数据，同时将查询请求广播至区块链网络中，使得全网在线的记账节点能够接收并各自进行本地查询，最后将查询结果进行共识。

[0148] 本实施例中，记账节点a接收到查询请求，查询到携带交易ID账户最新的10笔交易，此为本地节点a的查询结果。由于记账节点a已广播该查询请求，因而待接收其它记账节点反馈的查询结果，即接收到节点b、c、d...等的查询结果。假设当前区块链网络中处于在线的记账节点的总数 $N_{\text{总}}$ 为1000，当前调剂值 $T$ 为1，那么接收节点数计算可得501。若在预设时间内未接收到501个记账节点反馈的查询结果，则确定网络等待超时，即等待共识完成的时

长超过预设时长,向客户端下发查询失败以及网络等待超时的提示信息。若在预设时间内接收到501个记账节点反馈的查询结果时,即可执行共识计算,且计算的共识值大于或等于501,则说明目前所有记账节点超过50%以上的节点达成一致,即能够完成对本次查询账目的认可,此时向客户端返回共识一致的查询结果。若计算的共识值小于501则说明共识未达成一致,此时向客户端下发查询失败以及共识失败的提示信息。通过共识,将与共识一致的查询结果下发给客户端,保证数据的高可靠性,同时运算成本低,可降低资源消耗,提高效率。

[0149] 进一步可选的,为实现上述目的,本发明还提供一种计算机可读存储介质,在本实施例中提出的计算机可读存储介质上存储有账单处理程序,包括接收数据、执行对账和发起共识等。存储的账单处理程序能够被处理器读取、解读并执行,从而实现上述任一实施例中基于区块链数据库的账单处理方法的步骤。

[0150] 需要说明的是,在本文中,术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含,从而使得包括一系列要素的过程、方法、物品或者装置不仅包括那些要素,而且还包括没有明确列出的其他要素,或者是还包括为这种过程、方法、物品或者装置所固有的要素。在没有更多限制的情况下,由语句“包括一个……”限定的要素,并不排除在包括该要素的过程、方法、物品或者装置中还存在另外的相同要素。

[0151] 上述本发明实施例序号仅仅为了描述,不代表实施例的优劣。

[0152] 通过以上的实施方式的描述,本领域的技术人员可以清楚地了解到上述实施例方法可借助软件加必需的通用硬件平台的方式来实现,当然也可以通过硬件,但很多情况下前者是更佳的实施方式。基于这样的理解,本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来,该计算机软件产品存储在一个可读存储介质(如ROM/RAM、磁碟、光盘)中,包括若干指令用以使得一台终端(可以是手机,计算机,服务器,空调器,或者网络设备等)执行本发明各个实施例的方法。

[0153] 上面结合附图对本发明的实施例进行了描述,但是本发明并不局限于上述的具体实施方式,上述的具体实施方式仅仅是示意性的,而不是限制性的,本领域的普通技术人员在本发明的启示下,在不脱离本发明宗旨和权利要求所保护的范围情况下,还可做出很多形式,凡是利用本发明说明书及附图内容所作的等效结构或等效流程变换,或直接或间接运用在其他相关的技术领域,这些均属于本发明的保护之内。

[0154] 以上仅为本发明的优选实施例,并非因此限制本发明的专利范围,凡是利用本发明说明书及附图内容所作的等效结构或等效流程变换,或直接或间接运用在其他相关的技术领域,均同理包括在本发明的专利保护范围内。

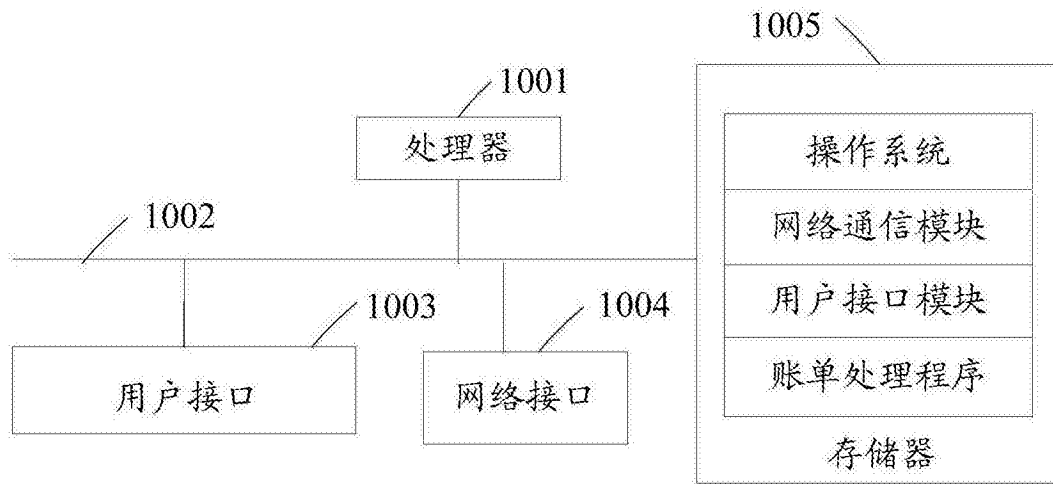


图1



图2

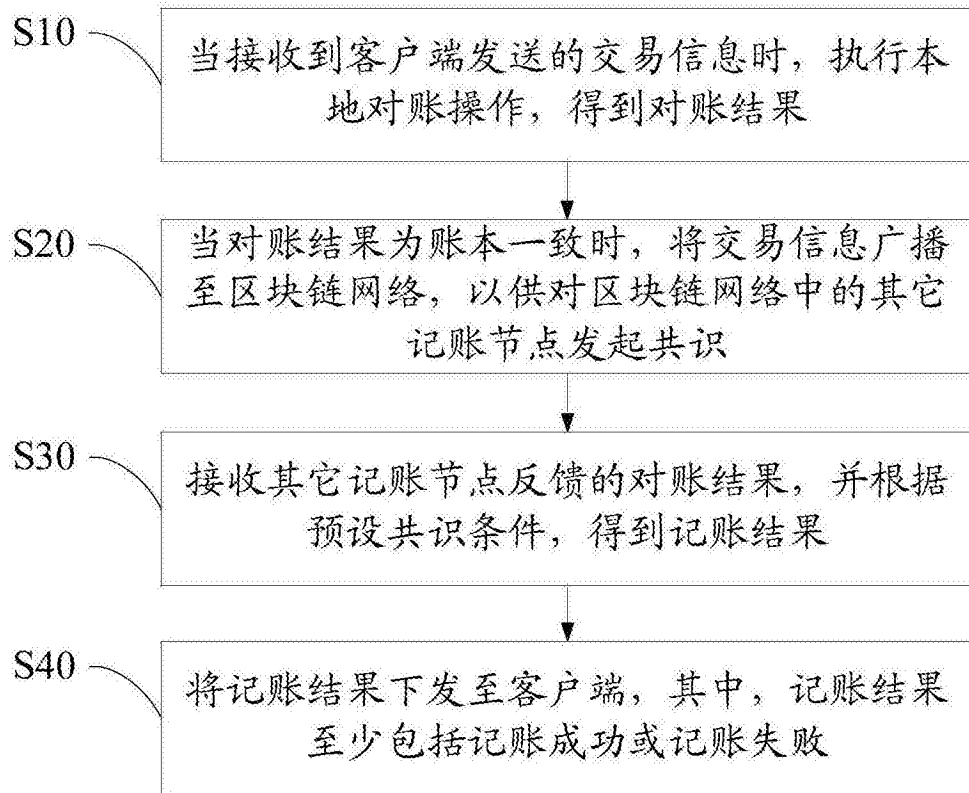


图3

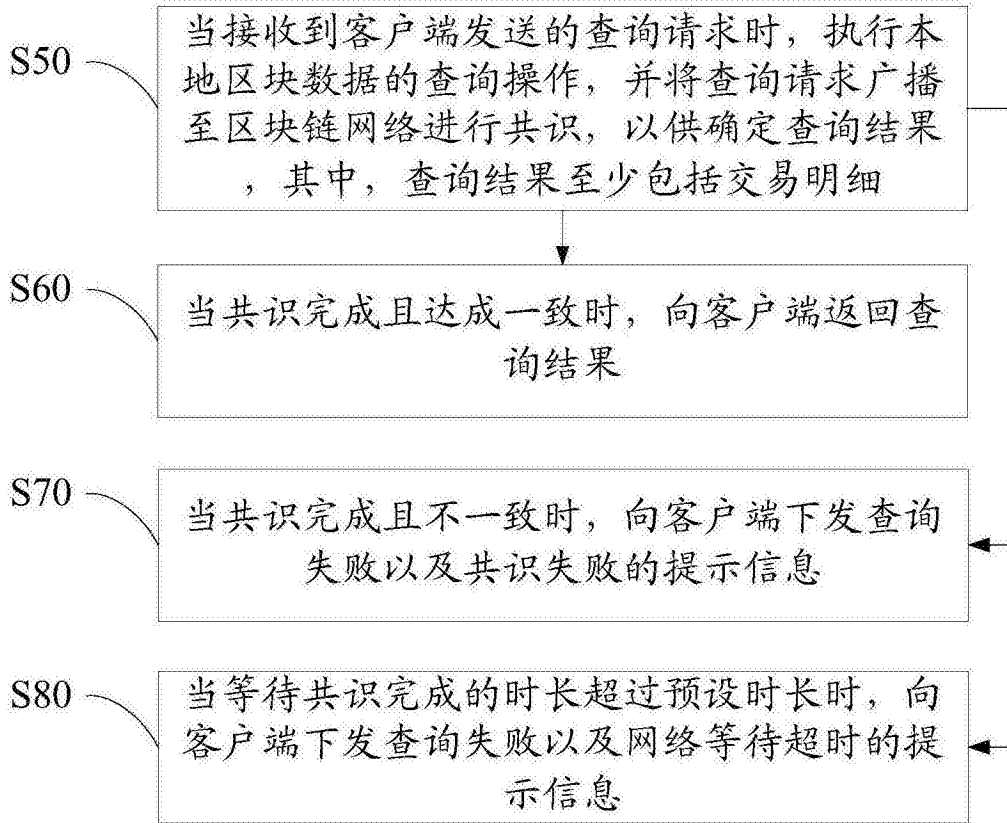


图4