(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 106845960 B
(45)授权公告日 2018.03.20

(21)申请号 201710060336.0

(22)申请日 2017.01.24

(65)同一申请的已公布的文献号
申请公布号 CN 106845960 A

(43)申请公布日 2017.06.13

(73)专利权人 上海壹账通区块链科技有限公司
地址 200000 上海市徐汇区龙腾大道2879号3楼3484室

(72)发明人 陆陈一帆 宦鹏飞 张宇 黄宇翔

(74)专利代理机构 深圳市沃德知识产权代理事务所(普通合伙) 44347
代理人 高杰 于志光

(51)Int.Cl.
G06F 19/00(2018.01)
G06Q 20/10(2012.01)
G06Q 20/38(2012.01)
H04L 9/00(2006.01)
H04L 9/32(2006.01)

(56)对比文件
CN 105931052 A,2016.09.07,
CN 105976232 A,2016.09.28,
US 9397985 B1,2016.07.19,
CN 106055993 A,2016.10.26,
CN 105956923 A,2016.09.21,
CN 105488665 A,2016.04.13,

审查员 朱云娥

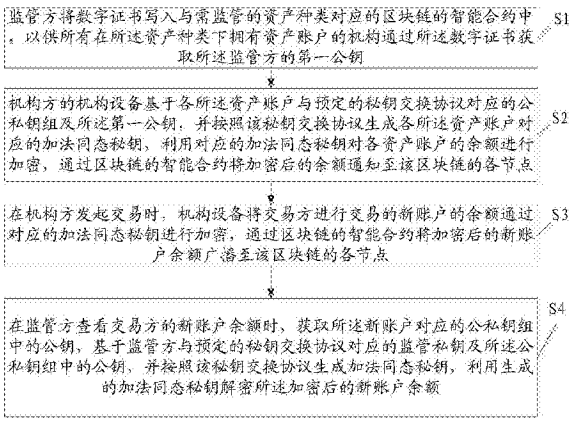
权利要求书3页 说明书10页 附图5页

(54)发明名称

基于区块链的安全交易方法及系统

(57)摘要

本发明涉及一种基于区块链的安全交易方法及系统，基于区块链的安全交易方法包括：监管方将其数字证书及其对应第一公钥写入与需监管的资产种类对应的区块链的智能合约中，以供所有在资产种类下拥有资产账户的机构通过数字证书获取监管方的第一公钥，以生成对资产账户的余额进行同态加密的加法同态秘钥；在监管方查看交易方的新账户的余额时，获取所述新账户对应的公私钥组中的公钥，基于监管方与预定的秘钥交换协议对应的监管私钥及所述公私钥组中的公钥，并按照该秘钥交换协议生成加法同态秘钥，利用生成的加法同态秘钥解密新账户加密后的新账户余额。本发明能有效保障了基于区块链的交易的账户安全性及对账户进行监管，并可提高交易处理的效率。



CN 106845960 B

1.一种基于区块链的安全交易方法，其特征在于，所述基于区块链的安全交易方法包括：

S1，监管方将数字证书写入与需监管的资产种类对应的区块链的智能合约中，以供所有在所述资产种类下拥有资产账户的机构通过所述数字证书获取所述监管方的第一公钥；

S2，机构方的机构设备基于该机构管理的各所述资产账户对应的公私钥组与预定的秘钥交换协议及所述第一公钥，并按照该秘钥交换协议生成各所述资产账户对应的加法同态秘钥，利用对应的加法同态秘钥对各资产账户的余额进行加密，通过区块链的智能合约将加密后的余额广播至该区块链的各节点的智能合约上；

S3，在机构方发起交易时，机构设备将交易方进行交易的新账户的余额通过对应的加法同态秘钥进行加密，通过区块链的智能合约将加密后的新账户余额广播至该区块链的各节点的智能合约上；

S4，在监管方查看交易方的新账户的余额时，获取所述新账户对应的公私钥组中的公钥，基于监管方与预定的秘钥交换协议对应的监管私钥及所述公私钥组中的公钥，并按照该秘钥交换协议生成加法同态秘钥，利用生成的加法同态秘钥解密所述加密后的新账户余额。

2.根据权利要求1所述的基于区块链的安全交易方法，其特征在于，所述步骤S4和S5可以被替换为：

S10，在机构方发起交易时，机构设备将交易方进行交易的资产账户的新余额通过对应的加法同态秘钥进行加密，通过区块链的智能合约将加密后的新余额广播至该区块链的各节点的智能合约上；

S11，在监管方查看交易方对应的资产账户的新余额时，获取所述账户对应的公私钥组中的公钥，基于监管方与预定的秘钥交换协议对应的监管私钥及所述公私钥组中的公钥，并按照该秘钥交换协议生成加法同态秘钥，利用生成的加法同态秘钥解密所述加密后的新余额。

3.根据权利要求1所述的基于区块链的安全交易方法，其特征在于，所述数字证书由证书认证机构基于所述监管方与预先确定的秘钥交换协议对应的第一公钥进行签名后生成，并颁发给监管方。

4.根据权利要求2或3所述的基于区块链的安全交易方法，其特征在于，所述步骤S3之后还包括：

S5，当区块链的节点接收到广播的各所述交易方对应的加密后的新账户余额后，启动各节点对应的智能合约进行合数验证；

S6，若各节点对应的智能合约分别对各所述交易方对应的加密后的新账户后余额的合数验证通过，则各节点对应的智能合约基于各所述交易方对应的加密后的新账户余额进行数据更新。

5.根据权利要求4所述的基于区块链的安全交易方法，其特征在于，所述步骤S5之后还包括：

S7，若有节点对应的智能合约对所述交易方对应的加密后的新账户余额的合数验证不通过，则向各参与合数验证的节点发送合数验证失败的通知，或者，向区块链上的所有节点发送合数验证失败的通知。

6.根据权利要求4所述的基于区块链的安全交易方法，其特征在于，所述步骤S6之后还包括：

S8，在监管方解密所述账户加密后的新账户余额后，启用负数余额验证系统对各所述交易方对应的解密后的新账户余额进行负数余额验证；

S9，若有资产账户未通过负数余额检验，则监管方将未通过负数余额检验的账户向除对应的异常节点外的其他节点进行通知，和/或，若有资产账户未通过负数余额检验，则监管方通过区块链权限管理系统取消未通过负数余额检验的账户在区块链上的交易权限。

7.一种基于区块链的安全交易系统，其特征在于，所述系统包括写入模块、第一加密模块、第二加密模块及解密模块，其中：

所述写入模块，用于将数字证书写入与需监管的资产种类对应的区块链的智能合约中，以供所有在所述资产种类下拥有资产账户的机构通过所述数字证书获取所述监管方的第一公钥；

所述第一加密模块基于当前机构管理的各所述资产账户对应的公私钥组中的私钥与预定的秘钥交换协议及所述第一公钥，并按照该秘钥交换协议生成各所述资产账户对应的加法同态秘钥，利用对应的加法同态秘钥对各资产账户的余额进行加密，通过区块链的智能合约将加密后的余额广播至该区块链的各节点的智能合约上；

所述第二加密模块在机构方发起交易时，将交易方进行交易的新账户的余额通过对应的加法同态秘钥进行加密，通过区块链的智能合约将加密后的新账户余额广播至该区块链的各节点的智能合约上；以及，

所述解密模块，用于在监管方查看交易方的账户的新账户余额时，获取所述新账户对应的公私钥组中的公钥，基于监管方与预定的秘钥交换协议对应的监管私钥及所述公私钥组中的公钥，并按照该秘钥交换协议生成加法同态秘钥，利用生成的加法同态秘钥解密所述账户加密后的新账户余额。

8.根据权利要求7所述的系统，其特征在于，所述数字证书由证书认证机构基于所述监管方与预先确定的秘钥交换协议对应的第一公钥进行签名后生成，并颁发给监管方。

9.根据权利要求7或8所述的系统，其特征在于，所述系统还包括：

第一验证模块，用于当区块链的节点接收到广播的各所述交易方对应的加密后的新账户余额后，启动各节点对应的智能合约进行合数验证；

更新模块，用于若各节点对应的智能合约分别对各所述交易方对应的加密后的新账户余额的合数验证通过，则各节点对应的智能合约基于各所述交易方对应的加密后的新账户余额进行数据更新。

10.根据权利要求9所述的系统，其特征在于，所述系统还包括：

发送模块，用于若有节点对应的智能合约对所述交易方对应的加密后的新账户余额的合数验证不通过，则向各参与合数验证的节点发送合数验证失败的通知，或者，向区块链上的所有节点发送合数验证失败的通知。

11.根据权利要求9所述的系统，其特征在于，所述系统还包括：

第二验证模块，用于在监管方解密所述加密后的新账户余额后，启用负数余额验证系统对各所述交易方对应的解密后的新账户余额进行负数余额验证；

处理模块，用于若有资产账户未通过负数余额检验，则监管方将未通过负数余额检验

的账户向除对应的异常节点外的其他节点进行通知，和/或，若有资产账户未通过负数余额检验，则监管方通过区块链权限管理系统取消未通过负数余额检验的账户在区块链上的交易权限。

基于区块链的安全交易方法及系统

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的安全交易方法及系统。

背景技术

[0002] 区块链技术具备去中心化、信息不可篡改性等特点，运用区块链技术可实现多方参与的交易事件(例如，转账交易、支付交易等)，例如，银行A与银行B在区块链上进行交易，那么该区块链上所有其他节点都会知晓这笔交易，其他参与方可以一起参与确认交易准确性，防止信息的篡改。然而，这种交易方式由于没有绝对权威机构节点，对每笔交易进行集体验证是必要的，其缺点在于：交易参与方的交易就会毫无私密可言，一个机构的账户有可能被其他节点上的机构跟踪，从而带来信息泄露的风险。

[0003] 为了解决上述问题，业内采用一种利用加法同态加密保护的方案，来解决区块链交易中信息泄露的问题。然而仍然存在不足之处：例如，当一个账户的账户余额受到加法同态加密保护后只有同态加密秘钥拥有方可以知晓该账户的实际余额，导致监管部门难以对金融资产流动性进行监管。如果要求资产拥有方通过某种形式把同态加密用秘钥传递给监管方，则会因为系统处理步骤复杂，导致容易出现错误及/或安全隐患，且效率低。

[0004] 综上所述，将区块链技术运用在交易场景下，并有效地保证交易信息的安全、交易处理的高效率及有效保证监管方对账户的监管，已成为亟待解决的技术问题。

发明内容

[0005] 本发明的目的在于提供一种基于区块链的安全交易方法及系统，旨在有效地保证基于区块链的交易的交易信息的安全、交易处理的高效率及有效保证监管方对账户的监管。

[0006] 为实现上述目的，本发明提供一种基于区块链的安全交易方法，所述基于区块链的安全交易方法包括：

[0007] S1，监管方将数字证书写入与需监管的资产种类对应的区块链的智能合约中，以供所有在所述资产种类下拥有资产账户的机构通过所述数字证书获取所述监管方的第一公钥；

[0008] S2，机构方的机构设备基于该机构管理的各所述资产账户对应的公私钥组与预定的秘钥交换协议及所述第一公钥，并按照该秘钥交换协议生成各所述资产账户对应的加法同态秘钥，利用对应的加法同态秘钥对各资产账户的余额进行加密，通过区块链的智能合约将加密后的余额广播至该区块链的各节点；

[0009] S3，在机构方发起交易时，机构设备将交易方进行交易的新账户的余额通过对应的加法同态秘钥进行加密，通过区块链的智能合约将加密后的新账户余额广播至该区块链的各节点；

[0010] S4，在监管方查看交易方的新账户余额时，获取所述新账户对应的公私钥组中的公钥，基于监管方与预定的秘钥交换协议对应的监管私钥及所述公私钥组中的公钥，并按

照该秘钥交换协议生成加法同态秘钥，利用生成的加法同态秘钥解密所述加密后的新账户余额。

[0011] 优选地，所述步骤S4和S5可以被替换为：

[0012] S10，在机构方发起交易时，机构设备将交易方进行交易的资产账户的新余额通过对应的加法同态秘钥进行加密，通过区块链的智能合约将加密后的新余额广播至该区块链的各节点的智能合约上；

[0013] S11，在监管方查看交易方对应的资产账户的新余额时，获取所述资产账户对应的公私钥组中的公钥，基于监管方与预定的秘钥交换协议对应的监管私钥及所述公私钥组中的公钥，并按照该秘钥交换协议生成加法同态秘钥，利用生成的加法同态秘钥解密所述加密后的新余额。

[0014] 优选地，所述数字证书由证书认证机构基于所述监管方与预先确定的秘钥交换协议对应的第一公钥进行签名后生成，并颁发给监管方。

[0015] 优选地，所述步骤S3之后还包括：

[0016] S5，当区块链的节点接收到广播的各所述交易方对应的加密后的新账户余额后，启动各节点对应的智能合约进行合数验证；

[0017] S6，若各节点对应的智能合约分别对各所述交易方对应的加密后的新账户余额的合数验证通过，则各节点对应的智能合约基于各所述交易方对应的加密后的新账户余额进行数据更新。

[0018] 优选地，所述步骤S5之后还包括：

[0019] S7，若有节点对应的智能合约对所述交易方对应的加密后的新账户余额的合数验证不通过，则向各参与合数验证的节点发送合数验证失败的通知，或者，向区块链上的所有节点发送合数验证失败的通知。

[0020] 优选地，所述步骤S6之后还包括：

[0021] S8，在监管方解密所述加密后的新账户余额后，启用负数余额验证系统对各所述交易方对应的解密后的新账户余额进行负数余额验证；

[0022] S9，若有资产账户未通过负数余额检验，则监管方将未通过负数余额检验的账户向除对应的异常节点外的其他节点进行通知，和/或，若有资产账户未通过负数余额检验，则监管方通过区块链权限管理系统取消未通过负数余额检验的账户在区块链上的交易权限。

[0023] 为实现上述目的，本发明还提供一种系统，所述系统包括：

[0024] 写入模块，用于将数字证书写入与需监管的资产种类对应的区块链的智能合约中，以供所有在所述资产种类下拥有资产账户的机构通过所述数字证书获取所述监管方的第一公钥，以生成对资产账户的余额及交易后的资产账户的新账户余额进行加密的加法同态秘钥；

[0025] 所述第一加密模块基于当前机构管理的各所述资产账户对应的公私钥组中的私钥与预定的秘钥交换协议及所述第一公钥，并按照该秘钥交换协议生成各所述资产账户对应的加法同态秘钥，利用对应的加法同态秘钥对各资产账户的余额进行加密，通过区块链的智能合约将加密后的余额广播至该区块链的各节点的智能合约上；

[0026] 所述第二加密模块在机构方发起交易时，将交易方进行交易的各资产账户的新账

户余额通过对应的加法同态秘钥进行加密，通过区块链的智能合约将加密后的新账户余额广播至该区块链的各节点的智能合约上；以及，

[0027] 所述解密模块，用于在监管方查看交易方的新账户的余额时，获取所述新账户对应的公私钥组中的公钥，基于监管方与预定的秘钥交换协议对应的监管私钥及所述公私钥组中的公钥，并按照该秘钥交换协议生成加法同态秘钥，利用生成的加法同态秘钥解密所述加密后的新账户余额。

[0028] 优选地，所述数字证书由证书认证机构基于所述监管方与预先确定的秘

[0029] 钥交换协议对应的第一公钥进行签名后生成，并颁发给监管方。

[0030] 优选地，所述系统还包括：

[0031] 第一验证模块，用于当区块链的节点接收到广播的各所述交易方对应的加密后的新账户余额后，启动各节点对应的智能合约进行合数验证；

[0032] 更新模块，用于若各节点对应的智能合约分别对各所述交易方对应的加密后的新账户余额的合数验证通过，则各节点对应的智能合约基于各所述交易方对应的加密后的新账户余额进行数据更新。

[0033] 优选地，所述系统还包括：

[0034] 发送模块，用于若有节点对应的智能合约对所述交易方对应的加密后的新账户余额的合数验证不通过，则向各参与合数验证的节点发送合数验证失败的通知，或者，向区块链上的所有节点发送合数验证失败的通知。

[0035] 优选地，所述系统还包括：

[0036] 第二验证模块，用于在监管方解密所述账户加密后的新账户余额后，启用负数余额验证系统对各所述交易方对应的解密后的新账户余额进行负数余额验证；

[0037] 处理模块，用于若有资产账户未通过负数余额检验，则监管方将未通过负数余额检验的账户向除对应的异常节点外的其他节点进行通知，和/或，若有资产账户未通过负数余额检验，则监管方通过区块链权限管理系统取消未通过负数余额检验的账户在区块链上的交易权限。

[0038] 本发明的有益效果是：本发明通过秘钥交换协议生成资产拥有方与监管方共同拥有的对称秘钥(即加法同态秘钥)，用该对称秘钥作为加法同态加密的加解密秘钥，这样监管方可以解密加密后的账户余额，其他无关方无法知晓该账户的实际余额，有效保障了账户安全性及对账户进行监管，并可提高交易处理的效率。

附图说明

[0039] 图1为本发明基于区块链的安全交易方法第一实施例的流程示意图；

[0040] 图2为本发明基于区块链的安全交易方法第二实施例的流程示意图；

[0041] 图3为本发明基于区块链的安全交易方法第三实施例的流程示意图；

[0042] 图4为本发明基于区块链的安全交易方法第四实施例的流程示意图；

[0043] 图5为本发明系统第一实施例的结构示意图；

[0044] 图6为本发明系统第二实施例的结构示意图；

[0045] 图7为本发明系统第三实施例的结构示意图。

具体实施方式

[0046] 以下结合附图对本发明的原理和特征进行描述，所举实例只用于解释本发明，并非用于限定本发明的范围。

[0047] 如图1所示，图1为本发明基于区块链的安全交易方法一实施例的流程示意图，该基于区块链的安全交易方法包括以下步骤：

[0048] 步骤S1，监管方将数字证书写入与需监管的资产种类对应的区块链的智能合约中，以供所有在所述资产种类下拥有资产账户的机构通过所述数字证书获取所述监管方的第一公钥。

[0049] 本实施例中，监管方将CA(Certification Authority，证书认证机构)颁发给自身的数字证书写入与需监管的资产种类对应的区块链的智能合约中，资产种类包括多种，例如，按耗用期限的长短，可分为流动资产和长期资产，根据具体形态，长期资产还可以作进一步的分类；按是否有实体形态，可分为有形资产和无形资产。或者综合几种分类标准，可将资产分为流动资产、长期投资、固定资产、无形资产、递延资产等类别。从这些资产类别中选择需要监管的资产种类。

[0050] 监管方将数字证书写入与需监管的资产种类对应的区块链的智能合约后，所有在需监管的资产种类下拥有资产账户的用户或机构(例如，金融机构、基金机构等)可以通过智能合约中写入的数字证书来获取监管方的第一公钥，该第一公钥供同态加密使用。

[0051] 另外，在监管方将数字证书写入与需监管的资产种类对应的区块链的智能合约之前，证书认证机构基于监管方与预先确定的秘钥交换协议对应的第一公钥进行签名，以生成数字证书，并颁发给监管方。

[0052] 步骤S2，机构方的机构设备基于该机构管理的各所述资产账户与预定的秘钥交换协议及所述第一公钥，并按照该秘钥交换协议生成各所述资产账户对应的加法同态秘钥，利用对应的加法同态秘钥对各资产账户的余额进行加密，通过区块链的智能合约将加密后的余额广播至该区块链的各节点；

[0053] 本实施例中，每一资产账户与预定的秘钥交换协议相对应，每一资产账户与预定的秘钥交换协议两者具有一对应的公私钥组，机构方的机构设备基于各资产账户与预定的秘钥交换协议(例如，Diffie-Hellman协议，国密SM2协议)对应的公私钥组及监管方的第一公钥，并按照该秘钥交换协议生成各资产账户对应的加法同态秘钥，具体地，首先获取公私钥组，然后获取公私钥组中的私钥，基于该私钥及监管方的第一公钥并按照该秘钥交换协议生成各资产账户对应的加法同态秘钥。

[0054] 其中，加法同态秘钥用作同态加密的加解密秘钥，该加法同态秘钥为对称秘钥(即发送和接收数据的双方必使用相同的秘钥对明文进行加密和解密运算)。

[0055] 机构方利用对应的加法同态秘钥对各资产账户的余额进行加密，例如，若一个用户或者机构在一个需监管的资产种类下有两个账户b1和b2，则b1账户的余额利用b1账户对应的加法同态秘钥进行加密；b2账户的余额利用b2账户对应的加法同态秘钥进行加密。最后，机构方将自己在需监管的资产种类下的各个账户进行同态加密后的余额通过区块链的智能合约通知至该区块链的各节点，具体地，将进行同态加密后的余额通过区块链的智能合约写到该区块链的各个节点上的共享资产账本上。

[0056] 其中，各资产账户的余额进行同态加密后，只有拥有加法同态秘钥的监管方及资产拥有方可以知晓对应的资产账户的余额。该资产账户可作为老用户，与下述的新用户对应。

[0057] 步骤S3，在机构方发起交易时，机构设备将交易方进行交易的新账户的余额通过对应的加法同态秘钥进行加密，通过区块链的智能合约将加密后的新账户余额广播至该区块链的各节点。

[0058] 本实施例中，用户或者机构可以创建新的资产账户进行交易，所创建的新的资产账户称为本实施例中的新账户，例如：在交易时，银行X把账号001上的100张票据变成400张，其可以在一个002账号并放上400余额，然后再创建一个新的003账号上存-300。002账号为账户余额经过同态加密后的资产账户，为上述的老账户，则003账号为新账户，其账户余额也经过同态加密。

[0059] 本实施例中，该区块链中的一个用户或者机构发起在上述的资产种类下的交易时，例如，A转账给B，该用户或机构把各个交易方进行交易的新账户的余额通过对应的各个交易方的资产账户加法同态秘钥进行同态加密，通过智能合约将各个交易方进行交易的同态加密后的新账户余额广播到该区块链的各个节点上，以便该区块链的各个节点上的其他用户或者机构能够知晓该交易(但无法知晓进行交易的新账户的余额)。

[0060] 步骤S4，在监管方查看交易方的新账户的余额时，获取所述新账户对应的公私钥组中的公钥，基于监管方与预定的秘钥交换协议对应的监管私钥及所述公私钥组中的公钥，并按照该秘钥交换协议生成加法同态秘钥，利用生成的加法同态秘钥解密所述加密后的新账户余额。

[0061] 监管方需要查看一个交易方的新账户的余额时，则监管方获取该交易方的新账户对应的公私钥组中的公钥，例如，通过智能合约获取广播来的该交易方的账户对应的公私钥组中的公钥，或者，该公钥本身就是对应的账户号的预先确定的部分(例如，该公钥可以是对应的账户号的第N1—N2号码段，N1和N2均为大于0的自然数)，利用监管方与预定的秘钥交换协议两者对应的监管私钥及账户对应的公私钥组中的公钥，并按照该秘钥交换协议生成加法同态秘钥，该生成的加法同态秘钥能够解密账户加密后的新账户余额。

[0062] 与现有技术相比，本实施例通过秘钥交换协议生成资产拥有方与监管方共同拥有的对称秘钥(即加法同态秘钥)，用该对称秘钥作为加法同态加密的加解密秘钥，这样监管方可以解密加密后的账户余额，其他无关方无法知晓该账户的实际余额，有效保障了账户安全性及对账户进行监管，并可提高交易处理的效率；另外，通过在区块链智能合约上部署监管方公钥及公开的秘钥交换协议参数，这样拥有或即将拥有该资产的用户可以根据监管方公钥及公开的秘钥交换协议参数生成只有该用户与监管方共有的同态加密秘钥，这样，在保证账户隐私性的同时，可以为不同智能合约上的不同类型资产设定不同的监管方，区块链的业务兼容性和业务扩展便捷性得到了很大的提升。

[0063] 在一优选地实施例中，如图2所示，步骤S3和S4可以分别替换为如下步骤S10和S11：

[0064] S10，在机构方发起交易时，机构设备将交易方进行交易的资产账户的新余额通过对应的加法同态秘钥进行加密，通过区块链的智能合约将加密后的新余额广播至该区块链的各节点的智能合约上；

[0065] S11，在监管方查看交易方对应的资产账户的新余额时，获取所述资产账户对应的公私钥组中的公钥，基于监管方与预定的秘钥交换协议对应的监管私钥及所述公私钥组中的公钥，并按照该秘钥交换协议生成加法同态秘钥，利用生成的加法同态秘钥解密所述加密后的新余额。

[0066] 该实施例与图1所示的实施例的区别在于，在该实施例中，交易方并未创建新的资产账户进行交易，而是使用已有的老账户进行交易，此时，进行交易后的账户余额相对于原余额而言即为新余额。该实施例中，对新余额的加密过程及解密过程等与图1所示的实施例一致，在此不再赘述。

[0067] 在一优选的实施例中，如图3所示，在上述图1的实施例的基础上，所述步骤S3之后还包括：

[0068] 步骤S5，当区块链的节点接收到广播的各所述交易方对应的加密后的新账户余额后，启动各节点对应的智能合约进行合数验证；

[0069] 步骤S6，若各节点对应的智能合约分别对各所述交易方对应的加密后的新账户余额的合数验证通过，则各节点对应的智能合约基于各所述交易方对应的加密后的新账户余额进行数据更新；

[0070] 步骤S7，若有节点对应的智能合约对所述交易方对应的加密后的新账户余额的合数验证不通过，则向各参与合数验证的节点发送合数验证失败的通知，或者，向区块链上的所有节点发送合数验证失败的通知。

[0071] 本实施例中，合数验证即验证交易前的所有节点的余额之和是否等于交易之后的所有节点的余额之和，例如：存在有效算法$\oplus$，使得$E(x+y)=E(x)\oplus E(y)$或者$x+y=D(E(x)\oplus E(y))$成立，该有效算法$\oplus$即为加法同态加密验证算法，这个算法在验证账户合数的同时，并不泄漏账户的余额x和y。

[0072] 若各节点对应的智能合约分别对各交易方对应的加密后的新账户余额的合数验证通过，则各节点对应的智能合约基于各交易方对应的加密后的新账户余额进行数据更新；若有节点对应的智能合约对交易方对应的加密后的新账户余额的合数验证不通过，则向各参与合数验证的节点发送合数验证失败的通知，或者，向区块链上的所有节点发送合数验证失败的通知。

[0073] 在一优选的实施例中，如图4所示，在上述图3的实施例的基础上，所述步骤S5之后还包括：

[0074] 步骤S8，在监管方解密所述加密后的新账户余额后，启用负数余额验证系统对各所述交易方对应的解密后的新账户余额进行负数余额验证；

[0075] 步骤S9，若有资产账户未通过负数余额检验，则监管方将未通过负数余额检验的账户向除对应的异常节点外的其他节点进行通知，和/或，若有资产账户未通过负数余额检验，则监管方通过区块链权限管理系统取消未通过负数余额检验的账户在区块链上的交易权限。

[0076] 本实施例中，由于同一个节点参与每次交易的账户和发生额是被记载在案的，所以通过虚假余额检验可以有效防止用户在某个节点通过分账户分摊余额的形式改变某个分账户的余额，从而规避合数验证的校验，例如，用户可以通过制造存有负数的账号来骗过验证：银行X把账号001上的100张票据变成400张：他可以创建一个002账号并放上400余额，

然后再在一个新的003账号上存-300，因此，需要进行负数余额验证。(注：负数在密码使用时一般是因为取摸(mod)溢出造成的，如当摸是300时，400mod 300就变成了100)

[0077] 如果各节点对应的智能合约分别对各交易方对应的加密后的新账户余额的合数验证通过，监管方对各个交易方对应的加密后的新账户余额进行解密，并在解密完毕后，启用负数余额验证系统对各个交易方对应的解密后的新账户余额进行负数余额验证，若有账户未通过负数余额检验，则监管方确定该账户，并将该账户的异常状况向除异常区块链节点外的其他节点进行通知，和/或，若有账户未通过负数余额检验，则监管方通过区块链权限管理系统取消异常账户在区块链上的交易权限。

[0078] 如图5所示，图5为本发明基于区块链的安全交易系统一实施例的结构示意图，该系统包括写入模块101、第一加密模块107、第二加密模块108及解密模块102。

[0079] 写入模块101，用于将数字证书写入与需监管的资产种类对应的区块链的智能合约中，以供所有在所述资产种类下拥有资产账户的机构通过所述数字证书获取所述监管方的第一公钥。

[0080] 本实施例中，监管方将CA(Certification Authority，证书认证机构)颁发给自身的数字证书写入与需监管的资产种类对应的区块链的智能合约中，资产种类包括多种，例如，按耗用期限的长短，可分为流动资产和长期资产，根据具体形态，长期资产还可以作进一步的分类；按是否有实体形态，可分为有形资产和无形资产。或者综合几种分类标准，可将资产分为流动资产、长期投资、固定资产、无形资产、递延资产等类别。从这些资产类别中选择需要监管的资产种类。

[0081] 监管方将数字证书写入与需监管的资产种类对应的区块链的智能合约后，所有在需监管的资产种类下拥有资产账户的用户或机构(例如，金融机构、基金机构等)可以通过智能合约中写入的数字证书来获取监管方的第一公钥，该第一公钥供同态加密使用。

[0082] 另外，在监管方将数字证书写入与需监管的资产种类对应的区块链的智能合约之前，证书认证机构基于监管方与预先确定的秘钥交换协议对应的第一公钥进行签名，以生成数字证书，并颁发给监管方。

[0083] 第一加密模块107，用于基于当前机构管理的各所述资产账户与预定的秘钥交换协议及所述第一公钥，并按照该秘钥交换协议生成各所述资产账户对应的加法同态秘钥，利用对应的加法同态秘钥对各资产账户的余额进行加密，通过区块链的智能合约将加密后的余额广播至该区块链的各节点。

[0084] 本实施例中，第一加密模块107可以设置于机构方的机构设备上。由于每一资产账户与预定的秘钥交换协议相对应，每一资产账户与预定的秘钥交换协议两者具有一对应的公私钥组，机构方的机构设备基于各资产账户与预定的秘钥交换协议(例如，Diffie-Hellman协议，国密SM2协议)对应的公私钥组及监管方的第一公钥，并按照该秘钥交换协议生成各资产账户对应的加法同态秘钥，具体地，首先获取公私钥组，然后获取公私钥组中的私钥，基于该私钥及监管方的第一公钥并按照该秘钥交换协议生成各资产账户对应的加法同态秘钥。

[0085] 其中，加法同态秘钥用作同态加密的加解密秘钥，该加法同态秘钥为对称秘钥(即发送和接收数据的双方必使用相同的秘钥对明文进行加密和解密运算)。

[0086] 机构方利用对应的加法同态秘钥对各资产账户的余额进行加密，例如，若一个用

户或者机构在一个需监管的资产种类下有两个账户b1和b2，则b1账户的余额利用b1账户对应的加法同态秘钥进行加密；b2账户的余额利用b2账户对应的加法同态秘钥进行加密。最后，机构方将自己在需监管的资产种类下的各个账户进行同态加密后的余额通过区块链的智能合约通知至该区块链的各节点，具体地，将进行同态加密后的余额通过区块链的智能合约写到该区块链的各个节点上的共享资产账本上。

[0087] 其中，各资产账户的余额进行同态加密后，只有拥有加法同态秘钥的监管方及资产拥有方可以知晓对应的资产账户的余额。该资产账户可作为老用户，与下述的新用户对应。

[0088] 第二加密模块108，用于在机构方发起交易时，将交易方进行交易的新账户的余额通过对应的加法同态秘钥进行加密，通过区块链的智能合约将加密后的新账户余额广播至该区块链的各节点。

[0089] 本实施例中，用户或者机构可以创建新的资产账户进行交易，所创建的新的资产账户称为本实施例中的新账户，例如：在交易时，银行X把账号001上的100张票据变成400张，其可以在一个002账号并放上400余额，然后再创建一个新的003账号上存-300。002账号为账户余额经过同态加密后的资产账户，为上述的老账户，则003账号为新账户，其账户余额也经过同态加密。

[0090] 本实施例中，第二加密模块108设置于机构方的机构设备上。当该区块链中的一个用户或者机构发起在上述的资产种类下的交易时，例如，A转账给B，该用户或机构把各个交易方进行交易的新账户的余额通过对应的各个交易方的资产账户加法同态秘钥进行同态加密，通过智能合约将各个交易方进行交易的同态加密后的新账户余额广播到该区块链的各个节点上，以便该区块链的各个节点上的其他用户或者机构能够知晓该交易(但无法知晓进行交易的新账户的余额)。

[0091] 解密模块102，用于在监管方查看交易方的新账户余额时，获取所述新账户对应的公私钥组中的公钥，基于监管方与预定的秘钥交换协议对应的监管私钥及所述公私钥组中的公钥，并按照该秘钥交换协议生成加法同态秘钥，利用生成的加法同态秘钥解密所述加密后的新账户余额。

[0092] 本实施例中，用户或者机构可以创建新的资产账户进行交易，所创建的新的资产账户称为本实施例中的新账户，例如：在交易时，银行X把账号001上的100张票据变成400张，其可以在一个002账号并放上400余额，然后再创建一个新的003账号上存-300。002账号为账户余额经过同态加密后的资产账户，为上述的老账户，则003账号为新账户，其账户余额也经过同态加密。

[0093] 监管方需要查看一个交易方的新账户的余额时，则监管方获取该交易方的新账户对应的公私钥组中的公钥，例如，通过智能合约获取广播来的该交易方的新账户对应的公私钥组中的公钥，或者，该公钥本身就是对应的账户号的预先确定的部分(例如，该公钥可以是对应的账户号的第N1—N2号码段，N1和N2均为大于0的自然数)，利用监管方与预定的秘钥交换协议两者对应的监管私钥及该公钥，并按照该秘钥交换协议生成加法同态秘钥，该生成的加法同态秘钥能够解密新账户余额。

[0094] 在一优选的实施例中，在进行交易时，交易方也可使用已有账户进行交易而非创建新账户进行交易，此时，第二加密模块108所加密的余额可以是已有账户在交易完成后的

新余额，而解密模块102所解密的余额相应地为已有账户在交易完成后的新余额。该实施例中，第二加密模块108对新余额的加密过程及解密模块102对新余额的解密过程等与图5所示的实施例一致，在此不再赘述。

[0095] 在一优选的实施例中，如图6所示，在上述图4的实施例的基础上，上述系统还包括：

[0096] 第一验证模块103，用于当区块链的节点接收到广播的各所述交易方对应的加密后的新账户余额后，启动各节点对应的智能合约进行合数验证；

[0097] 更新模块104，用于若各节点对应的智能合约分别对各所述交易方对应的加密后的新账户余额的合数验证通过，则各节点对应的智能合约基于各所述交易方对应的加密后的新账户余额进行数据更新。

[0098] 本实施例中，合数验证即验证交易前的所有节点的余额之和是否等于交易之后的所有节点的余额之和，例如：存在有效算法⊕，使得E(x+y)＝E(x)⊕E(y)或者x+y＝D(E(x)⊕E(y))成立，该有效算法⊕即为加法同态加密验证算法，这个算法在验证账户合数的同时，并不泄漏账户的余额x和y。

[0099] 若各节点对应的智能合约分别对各交易方对应的加密后的新账户余额的合数验证通过，则各节点对应的智能合约基于各交易方对应的加密后的新账户余额进行数据更新。

[0100] 优选地，还包括发送模块，用于若有节点对应的智能合约对所述交易方对应的加密后的新账户余额的合数验证不通过，则向各参与合数验证的节点发送合数验证失败的通知，或者，向区块链上的所有节点发送合数验证失败的通知。

[0101] 在一优选的实施例中，如图7所示，在上述图6的实施例的基础上，上述系统还包括：

[0102] 第二验证模块105，用于在监管方解密所述新账户加密后的新账户余额后，启用负数余额验证系统对各所述交易方对应的解密后的新账户余额进行负数余额验证；

[0103] 处理模块106，用于若有资产账户未通过负数余额检验，则监管方将未通过负数余额检验的账户向除对应的异常节点外的其他节点进行通知，和/或，若有资产账户未通过负数余额检验，则监管方通过区块链权限管理系统取消未通过负数余额检验的账户在区块链上的交易权限。

[0104] 本实施例中，由于同一个节点参与每次交易的账户和发生额是被记载在案的，所以通过虚假余额检验可以有效防止用户在某个节点通过分账户分摊余额的形式改变某个分账户的余额，从而规避合数验证的校验，例如，用户可以通过制造存有负数的账号来骗过验证：银行X把账号001上的100张票据变成400张：他可以创建一个002账号并放上400余额，然后再在一个新的003账号上存-300，因此，需要进行负数余额验证。

[0105] 如果各节点对应的智能合约分别对各交易方对应的加密后的新账户余额的合数验证通过，监管方对各个交易方对应的加密后的新账户余额进行解密，并在解密完毕后，启用负数余额验证系统对各个交易方对应的解密后的新账户余额进行负数余额验证，若有账户未通过负数余额检验，则监管方确定该账户，并将该账户的异常状况向除异常区块链节点外的其他节点进行通知，和/或，若有账户未通过负数余额检验，则监管方通过区块链权限管理系统取消异常账户在区块链上的交易权限。

[0106] 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。

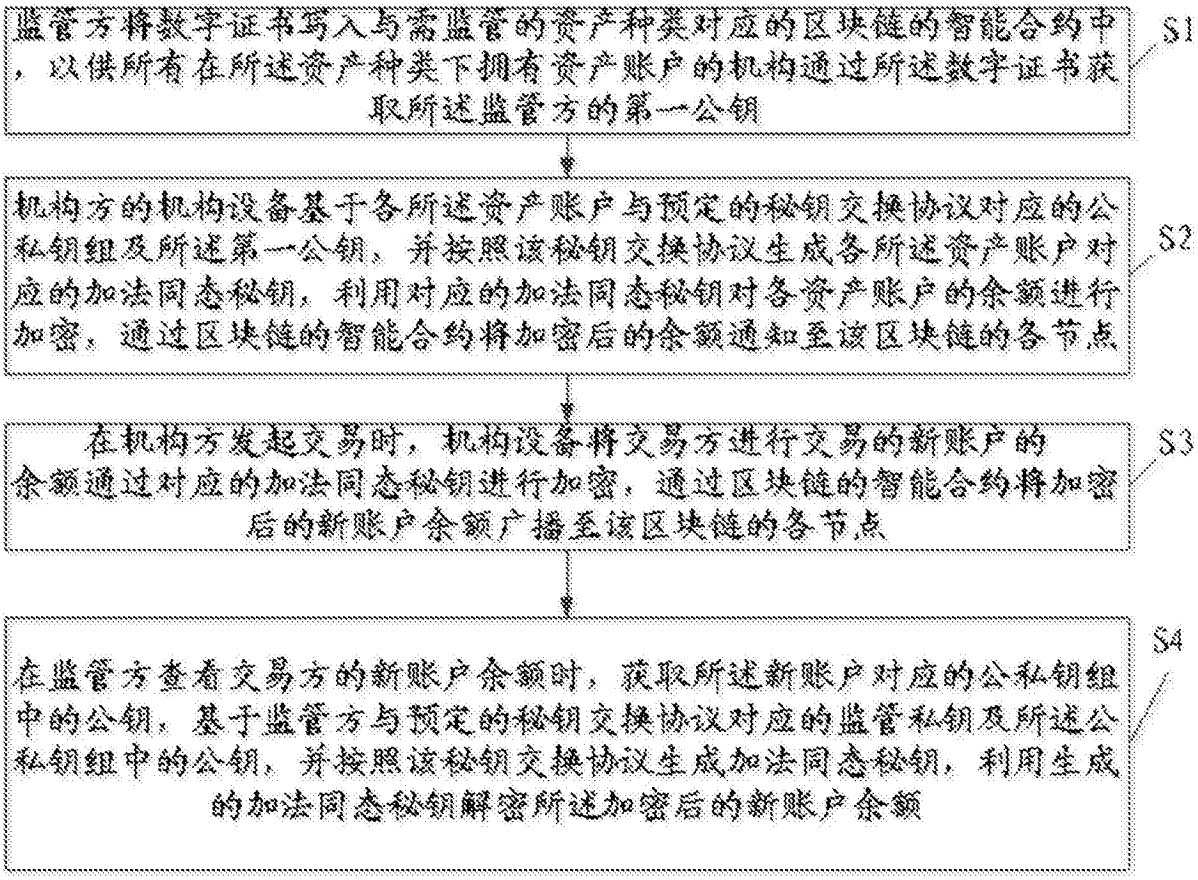

监管方将数字证书写入与需监管的资产种类对应的区块链的智能合约中，以供所有在所述资产种类下拥有资产账户的机构通过所述数字证书获取所述监管方的第一公钥
S1
机构方的机构设备基于各所述资产账户与预定的秘钥交换协议对应的公私钥组及所述第一公钥，并按照该秘钥交换协议生成各所述资产账户对应的加法同态秘钥，利用对应的加法同态秘钥对各资产账户的余额进行加密，通过区块链的智能合约将加密后的余额通知至该区块链的各节点
S2
在机构方发起交易时，机构设备将交易方进行交易的新账户的余额通过对应的加法同态秘钥进行加密，通过区块链的智能合约将加密后的新账户余额广播至该区块链的各节点
S3
在监管方查看交易方的新账户余额时，获取所述新账户对应的公私钥组中的公钥，基于监管方与预定的秘钥交换协议对应的监管私钥及所述公私钥组中的公钥，并按照该秘钥交换协议生成加法同态秘钥，利用生成的加法同态秘钥解密所述加密后的新账户余额
S4

图1

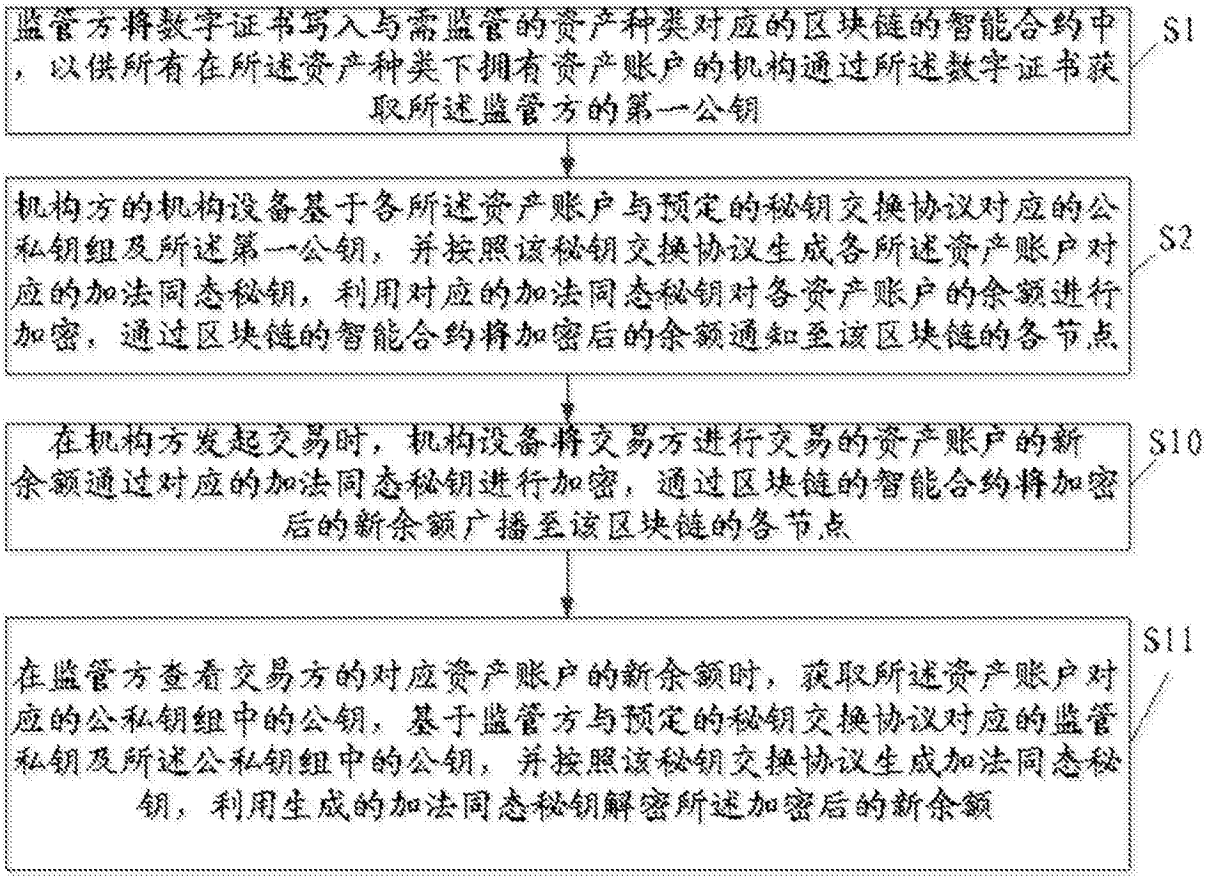

监管方将数字证书写入与需监管的资产种类对应的区块链的智能合约中，以供所有在所述资产种类下拥有资产账户的机构通过所述数字证书获取所述监管方的第一公钥
S1
机构方的机构设备基于各所述资产账户与预定的秘钥交换协议对应的公私钥组及所述第一公钥，并按照该秘钥交换协议生成各所述资产账户对应的加法同态秘钥，利用对应的加法同态秘钥对各资产账户的余额进行加密，通过区块链的智能合约将加密后的余额通知至该区块链的各节点
S2
在机构方发起交易时，机构设备将交易方进行交易的资产账户的新余额通过对应的加法同态秘钥进行加密，通过区块链的智能合约将加密后的新余额广播至该区块链的各节点
S10
在监管方查看交易方的对应资产账户的新余额时，获取所述资产账户对应的公私钥组中的公钥，基于监管方与预定的秘钥交换协议对应的监管私钥及所述公私钥组中的公钥，并按照该秘钥交换协议生成加法同态秘钥，利用生成的加法同态秘钥解密所述加密后的新余额
S11

图2

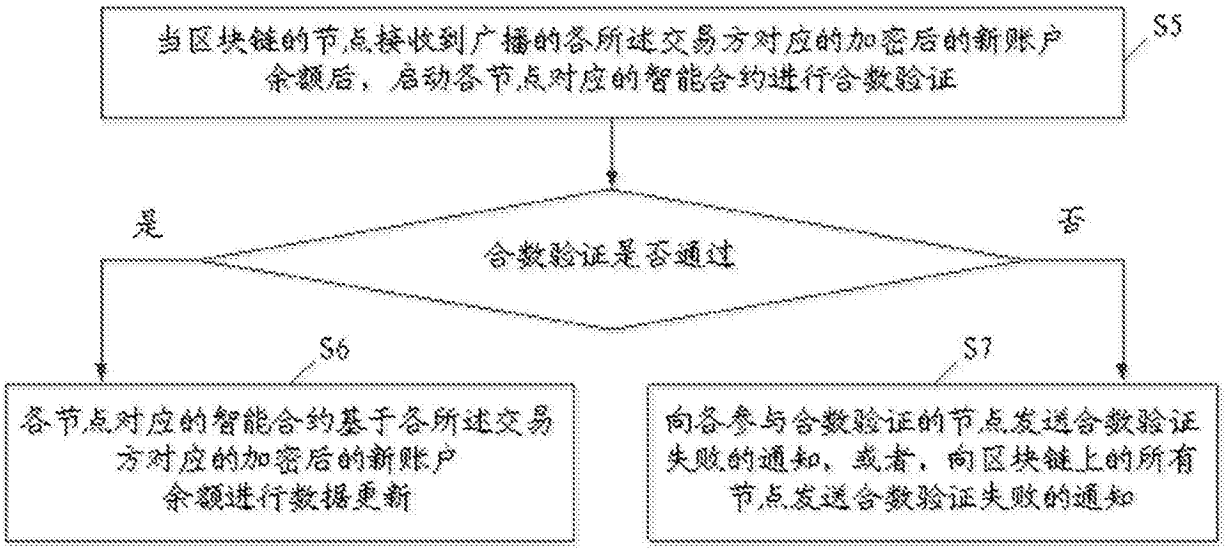

当区块链的节点接收到广播的各所述交易方对应的加密后的新账户余额后，启动各节点对应的智能合约进行合数验证
S5
合数验证是否通过
是
否
S6
各节点对应的智能合约基于各所述交易方对应的加密后的新账户余额进行数据更新
S7
向各参与合数验证的节点发送合数验证失败的通知，或者，向区块链上的所有节点发送合数验证失败的通知

图3

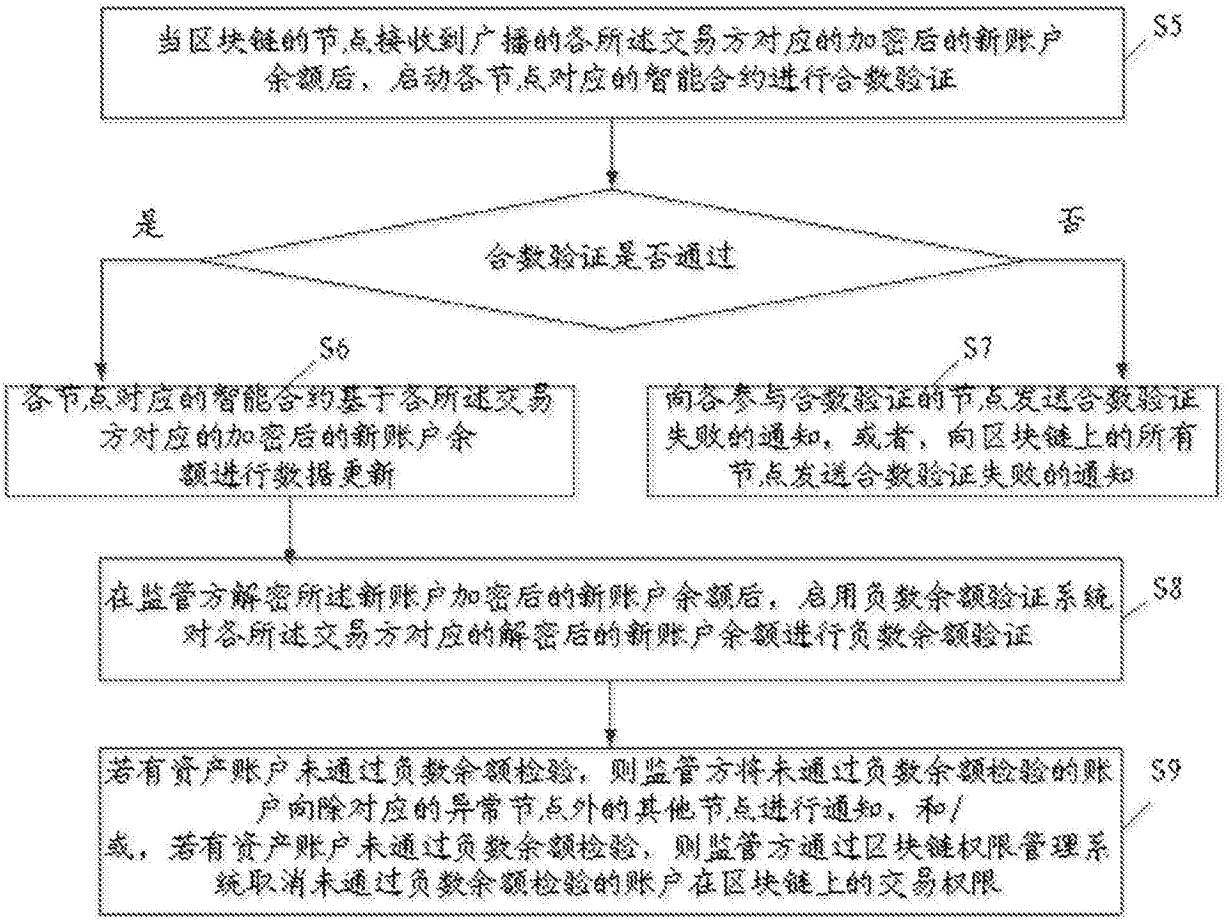

当区块链的节点接收到广播的各所述交易方对应的加密后的新账户余额后，启动各节点对应的智能合约进行合数验证
S5
是
否
合数验证是否通过
S6
S7
各节点对应的智能合约基于各所述交易方对应的加密后的新账户余额进行数据更新
向各参与合数验证的节点发送合数验证失败的通知，或者，向区块链上的所有节点发送合数验证失败的通知
在监管方解密所述新账户加密后的新账户余额后，启用负数余额验证系统对各所述交易方对应的解密后的新账户余额进行负数余额验证
S8
若有资产账户未通过负数余额检验，则监管方将未通过负数余额检验的账户向除对应的异常节点外的其他节点进行通知，和/或，若有资产账户未通过负数余额检验，则监管方通过区块链权限管理系统取消未通过负数余额检验的账户在区块链上的交易权限
S9

图4

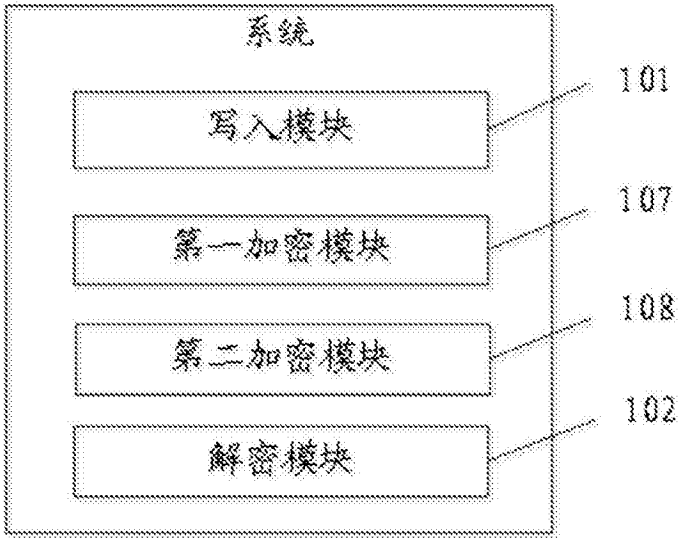

系统
写入模块
101
第一加密模块
107
第二加密模块
108
解密模块
102

图5

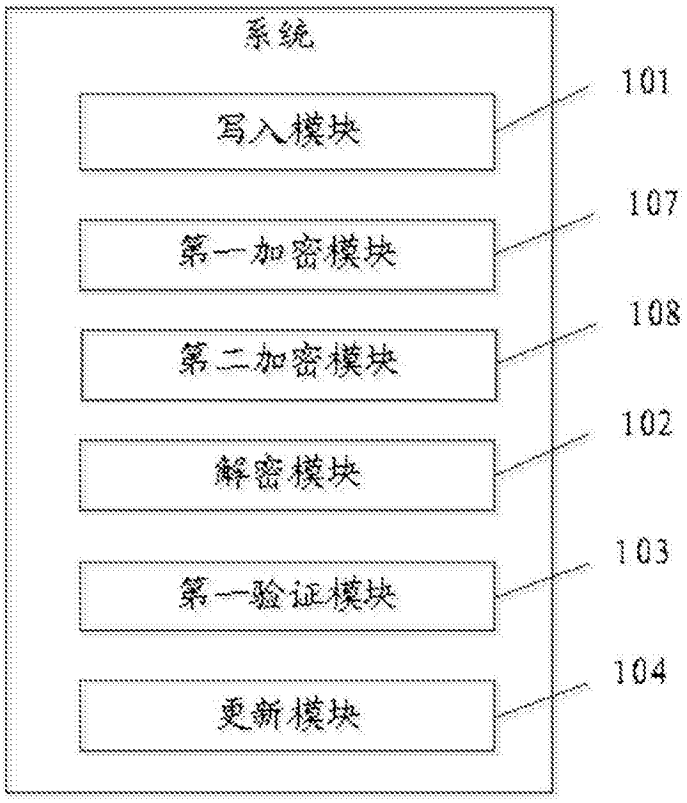

系统
写入模块
101
第一加密模块
107
第二加密模块
108
解密模块
102
第一验证模块
103
更新模块
104

图6

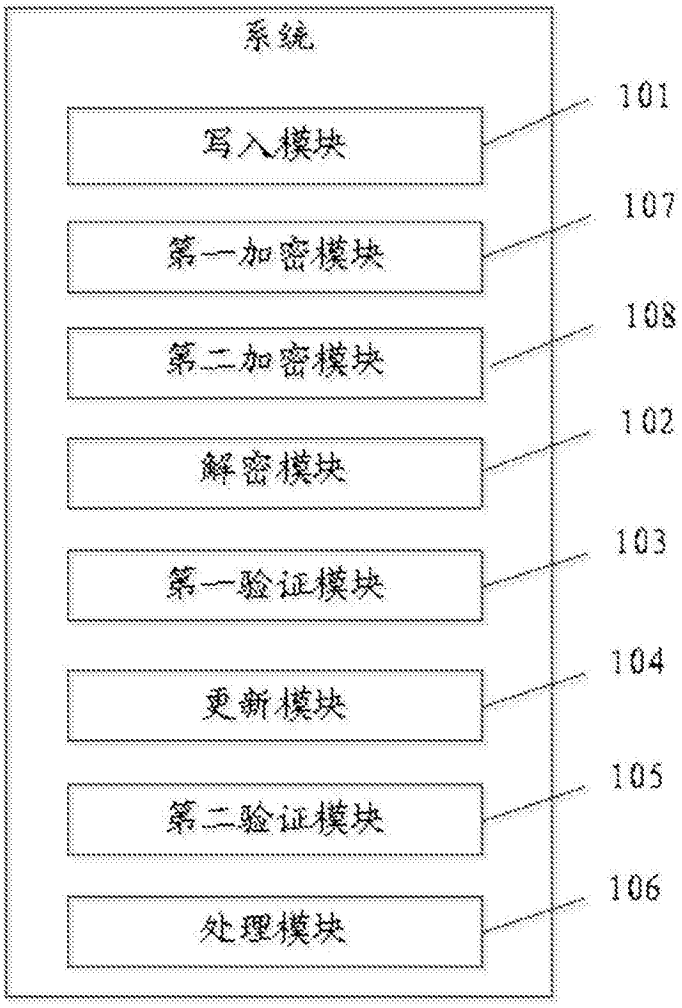

系统
写入模块
101
第一加密模块
107
第二加密模块
108
解密模块
102
第一验证模块
103
更新模块
104
第二验证模块
105
处理模块
106

图7